CONFINDUSTRIA

Response to the consultation on the European Data Protection Board Guidelines on the processing of personal data for scientific research purposes

Position Paper

25 June 2026

1. Introduction

Confindustria is the leading organisation representing manufacturing and service enterprises in Italy. Its confederal membership system represents more than 151,000 enterprises, reflecting the various industrial and productive sectors of the country. The Association promotes and protects the interests of the Italian productive system, contributing to the dialogue with national, European and international institutions on the industrial, economic and regulatory policies relevant to the competitiveness of enterprises, innovation, sustainable growth and the development of the country.

Confindustria welcomes the initiative of the European Data Protection Board (EDPB), aimed at providing interpretative clarifications on the processing of personal data for scientific research purposes under Regulation (EU) 2016/679 (GDPR). A uniform and predictable application of the GDPR in the field of scientific research is, indeed, essential to reconcile the protection of fundamental rights with the need to support European technological and industrial innovation.

Industrial research and experimental development are indispensable components of the European research ecosystem. In the fields of life sciences, artificial intelligence, advanced manufacturing, automation, security, energy and sustainability, the responsible use of personal data can make a decisive contribution to the development of technological, therapeutic and organisational solutions of general interest.

For this reason, it is essential that the interpretation and application of the provisions relevant to scientific research ensure an effective balance between the protection of personal data, the freedom of research and the European objectives of competitiveness, strategic autonomy and innovation. An excessively restrictive or formalistic approach would, in fact, risk producing effects contrary to the objectives pursued by the European legislator, holding back investment, cross-border collaboration, public-private partnerships and the development of new technologies.

This need is particularly significant at the present time, marked by a profound evolution of the European regulatory framework on the generation, access, sharing and re-use of data, including personal data. It is, therefore, essential that the Guidelines are positioned consistently with this evolution, also in light of the new European Strategy for the Data Union, Regulation (EU) 2024/1689 (the AI Act), Regulation (EU) 2025/327 (the European Health Data Space) and, prospectively, the Digital Omnibus and the Biotech Act. Effective coordination among these instruments is necessary in order to avoid interpretative misalignments that could generate uncertainty for enterprises and hinder the availability and responsible use of data for research and innovation purposes.

Overall, Confindustria takes a positive view of several aspects of the Guidelines, which help outline a clearer interpretative framework that is more closely aligned with the needs of scientific research, innovation and the competitiveness of the productive system.

The first aspect is the **definition of scientific research**. The Guidelines, indeed, emphasise how the GDPR has already adopted a broad concept of such activity (Recital 159), reiterating in several places that it may also be carried out by private entities and pursue commercial purposes.

This is particularly significant, as it reflects the evolution of the contemporary research model, increasingly based on the interaction between public and private actors, academic expertise, industrial capabilities and technological infrastructures. In this context, industry plays an essential role not only in funding research activities, but also in transforming the knowledge acquired into concrete applications, through the development of innovative products, services, processes and solutions capable of generating benefits for citizens, enterprises, public administrations and, more generally, for society as a whole.

The explicit recognition of the possible commercial dimension of scientific research therefore represents an important element, as it helps to clarify the boundaries of lawful processing of personal data carried out for such purposes and to reduce interpretative uncertainties which, in the absence of adequate guidance, could hinder legitimate initiatives of innovation, experimentation and technological development.

Equally positive are the indications relating to the **presumption of compatibility of further processing for research purposes** and to the possibility of **storing personal data** for longer periods, where this is necessary for the pursuit of specific scientific purposes and accompanied by appropriate safeguards.

These are essential aspects, since scientific research, especially in sectors with a higher technological and regulatory intensity, often requires the possibility of re-using and storing data over time, in order to ensure the continuity, verifiability and robustness of results. This need is particularly evident in longitudinal projects, in the validation and reproducibility of outcomes, in regulatory traceability, in pharmacovigilance and in *post-market* surveillance.

It is, moreover, positive that the following may also be brought within scientific research purposes: **ancillary processing operations**, such as the identification of relevant data, extraction, filtering, grouping, curation and categorisation of personal data, as well as their anonymisation and pseudonymisation. This is considerably useful at a practical level, since these activities, although not coinciding with scientific analysis in the strict sense, often constitute a necessary precondition for it. This is particularly true for industrial and applied research, where the collection, selection, normalisation and structuring of data represent essential steps to ensure the quality, consistency and reliability of research processes and results. It is, therefore, appropriate that the Guidelines expressly confirm this approach.

Confindustria also appreciates the EDPB's effort to identify **examples of appropriate safeguards**, which may serve as a useful operational reference for enterprises, research bodies and competent authorities. If applied in a consistent and proportionate manner, such indications can contribute to building a more integrated, competitive and reliable European Research Area, reducing the risk of divergent interpretations and fragmented approaches among Member States that may penalise the innovative capacity of the European Union.

Likewise, the attention that the Guidelines devote to technological evolution is appreciated, through the recognition, among the possible safeguards, of so-called **privacy-enhancing technologies** (PETs), including those based on synthetic data and homomorphic encryption techniques. This openness makes it possible to calibrate protective measures to state-of-the-art and to the most advanced technological solutions, reconciling data protection with the capacity for innovation and promoting a dynamic approach, suitable for incorporating technical progress with a view to the effective reduction of re-identification risks.

It is also positive that, among the possible safeguards, recognition is given to **codes of conduct**, as instruments that enhance the accountability of enterprises and guide their *compliance* activities.

At the same time, certain aspects remain that require greater attention and further refinement in the final version of the Guidelines.

This concerns, in particular, the criteria for qualifying scientific research, the application of legitimate interest as a legal basis for processing, the proportionality of the safeguards required, the definition of data protection roles, the risk of fragmentation arising from national rules and the need to take adequate account of the specific features of industrial, applied and cross-border research.

These aspects are decisive in ensuring that the European interpretative framework does not result in excessive burdens or in application uncertainties.

It therefore remains essential to promote an approach based on risk and on the concrete features of the processing operations, while maintaining a proportionate, technologically neutral approach that is consistent with the evolving European regulatory framework.

In light of these considerations, set out below are some detailed observations on the aspects of the Guidelines that are of greatest relevance for enterprises and for the development of industrial research and innovation.

2. Detailed observations

2.1 Processing of personal data for scientific research purposes (Section 2)

The Guidelines identify six key criteria for determining whether processing is motivated by scientific research purposes. Confindustria shares the need to prevent purely commercial, *marketing* or profiling activities from being improperly brought within this scope. However, some of the criteria referred to, if interpreted rigidly, risk anchoring the notion of scientific research to a model that is not fully aligned with the dynamics of industrial R&D and experimental development.

In particular, the verifiability of results through peer-reviewed publications (*peer review*), as well as the reference to the qualifications of the personnel involved, should not be given a predominant weight, nor should they in practice translate into necessary requirements for qualifying the activity as scientific research. With regard to the latter aspect, it is necessary to avoid the holding of formal academic titles or predetermined specialist qualifications being regarded as the only relevant indicator of the scientific or technical competence of the personnel engaged in the research.

In industrial R&D, indeed, methodological rigour and the reliability of results can also be ensured through specialist expertise acquired in professional, technical, regulatory or production settings, as well as through the organisation of multidisciplinary *teams* endowed with the expertise required in relation to the nature of the project. In many sectors, the quality of research depends not only on academic profiles, but also on applied experience, knowledge of processes, engineering capabilities, in addition to clinical, regulatory, IT, statistical, quality and safety competences.

Similarly, the scientific nature of the activity may be demonstrated through indicators other than traditional academic publication. Consider, for example, methodological documentation, experimental traceability, technical validation, compliance with regulatory and quality standards, the passing of audits, product certification, the filing of patent applications, as well as the preparation of technical, clinical or regulatory *dossiers*.

It is, therefore, necessary that the criteria identified be **supplemented with elements more closely aligned with the features of industrial research and experimental development**, giving weight to the degree of technological maturity of the project, the robustness of the method adopted, validation activities and compliance with applicable *standards*.

Similar caution is called for with regard to the criterion of autonomy and independence. Confindustria shares the need to preserve the integrity of scientific activity, to prevent undue interference and to ensure the reliability of results. However, this criterion too, if interpreted in excessively restrictive terms, risks failing to reflect adequately the specific features of industrial R&D.

In the industrial context, research is often linked to objectives of investment, product development, technology transfer and competitiveness. In light of these features, it would be appropriate to **clarify that the presence of commercial purposes, of private funding or of intellectual property protection needs does not, in itself, constitute an indication of a lack of autonomy or independence, nor an element capable of calling into question the scientific qualification of the activity** surveillance.

The assessment should, instead, focus on the presence of adequate safeguards for methodological and scientific integrity, such as the robustness of protocols, the quality and validation of data, the traceability of decisions, the management of any conflicts of interest, as well as the adoption of security and *accountability* measures proportionate to the risks of the processing.

A further aspect concerns the **manner of application of the six criteria**. In particular, where research activities do not fully satisfy such factors, the Guidelines provide that the controller must justify and be able to demonstrate the reasons why the activities concerned may nonetheless qualify as scientific research within the meaning of the GDPR.

On this point, it would be appropriate to clarify that such **factors are indicative and neither exhaustive nor cumulative in nature**, and that their application must be based on an overall assessment that is proportionate and tailored to the features of the specific case. Such a clarification would be consistent with the notion of scientific research adopted in Recital 159 GDPR, which expressly includes “technological development and demonstration, fundamental research, applied research and privately funded research”, in line with the Union’s objective of achieving a European Research Area, pursuant to Article 179 TFEU.

In the absence of such a clarification, the six factors could be applied, in practice, as a cumulative test or as a list of necessary requirements, making it more burdensome to qualify as scientific those activities which, although falling within the scope of Recital 159 and complying with the *standards* methodological standards of the relevant sector, do not necessarily display all the elements indicated.

This may occur, for example, in certain applied research and experimental development activities, which are not always intended for public disclosure or for publication in peer-reviewed outlets. In such contexts, the non-publication of results may be due to legitimate reasons, such as the protection of trade secrets or intellectual property, security, industrial confidentiality or competitive advantage, without this necessarily affecting the methodological rigour or the scientific nature of the activity carried out.

In such cases, an excessively burdensome demonstrative requirement on controllers could result in a disproportionate burden for private operators, introducing in practice a differentiation not provided for by the GDPR. The Regulation, indeed, does not make the qualification of scientific research conditional on the public or private, profit or non-profit nature of the entities involved, nor does it require the activity necessarily to display all the indicators identified by the Guidelines.

It would, therefore, be appropriate to clarify that the absence of one or more factors does not, in itself, affect the scientific qualification of the activity, which should be assessed on a substantive basis.

2.2 Research data infrastructures (Section 2.2)

Confindustria shares the recognition that personal data may be processed in a research data infrastructure (repository or research database) in order to make them available to future projects within a specific area of research. Such infrastructures - including federated and public-private infrastructures - represent, indeed, a strategic asset for the competitiveness of European research across all sectors.

The possibility of making personal data available for future projects in a given scientific field is essential to make the most of existing datasets, avoid duplication, reduce costs and accelerate the development of new knowledge and innovative solutions. This is particularly relevant with regard to federated research infrastructures, which allow the analysis of data distributed across different entities or systems, without imposing unnecessary transfers or centralisation.

It is, therefore, appropriate that the Guidelines promote such infrastructures with a view to interoperability with sectoral data spaces (for example, the European Health Data Space) and clarify that they **may include heterogeneous categories of data** - including, where relevant and with appropriate safeguards, special categories of data such as genetic data - without prejudice to the need to ensure appropriate safeguards, including high levels of IT security, secure processing environments, role-based access controls, traceability of access and rigorous governance of data use.

It would, moreover, be appropriate for the Guidelines to include an explicit reference to **federated infrastructures**, security requirements and the *governance* of access, in coordination with the European data spaces. In particular, it should be clarified that the establishment and operation of data infrastructures for research may themselves constitute scientific research purposes, where research areas, access criteria, appropriate technical and organisational measures, controls on use and conditions for further processing are defined.

Finally, the Guidelines should **promote federated and secure models of data access**, suitable for allowing analyses to be carried out without unnecessary transfers and with appropriate control measures. To this end, relevance is attached to secure processing environments, role-based access controls, traceability of access, high levels of IT security, authorisation procedures and rigorous governance of data use, consistently with the principle of data minimisation and with the need to facilitate cross-border research.

2.3 Legal bases and consent (Section 4)

2.3.1 Broad consent and dynamic consent (Section 4.1.2)

Confindustria welcomes the indications of the Guidelines on broad consent and dynamic consent, as useful tools in research projects characterised by progressive purposes and developments, in which the future uses of the data are not always entirely foreseeable at the time of the initial collection.

Moreover, significant difficulties arise for operators carrying out research activities where retrospective studies are subsequently defined and must involve a high number of patients per individual centre, with the result that providing for a generic consent, not specific to the individual project — however detailed as to its purposes and accompanied by appropriate safeguards and information measures — would facilitate this important scientific research activity.

With regard to **broad consent**, the Guidelines provide that controllers relying on broad consent must "ensure that data subjects understand the consequence of their choice", namely that their personal data will be processed within research projects falling within the scientific research area communicated to them.

While sharing the objective of safeguarding the autonomy of data subjects, it is considered that this wording sets an unworkable standard. The controller can and must share information in a clear, concise, transparent and intelligible form, in accordance with Article 12(1) GDPR, and make such information effectively accessible; it cannot, however, be required to ascertain the subjective level of understanding actually attained by each data subject.

It would, therefore, be appropriate to clarify that the controller's obligation consists in making available adequate information on the consequences of the choice, in a manner apt to facilitate its understanding, **without transforming that obligation into an individual verification of the data subject's actual understanding** of surveillance.

Similar proportionality requirements apply to the safeguards indicated for broad consent, including use and access control measures (such as an independent data trustee), the time-limited validity of consent or an independent oversight body.

While recognising the usefulness of such measures for the protection of data subjects, it is observed that some of them entail significant organisational, economic and procedural burdens for individual enterprises. Setting up an independent data trustee or an independent oversight body - composed of representatives of the data subjects, experts in the relevant research field, data protection experts and, where designated, the data protection officer - presupposes, indeed, structures, resources and processes that are more easily sustainable

by entities operating on a large scale or in aggregated form, such as biobanks, research infrastructures and Real World Evidence *(RWE)* databases. Their undifferentiated application could, therefore, result in a disproportionate burden, in particular for smaller enterprises or for more limited research projects, thereby discouraging research.

It would, therefore, be necessary to **clarify that the safeguards indicated for broad consent constitute options to be calibrated** according to the nature, scope, context and risks of the processing, as well as the size and characteristics of the controller, and not a cumulative set of measures of general application.

A further issue concerns the **practical effects of the distinction between consent to participate in a research activity**, required by ethical, health or regulatory rules, and consent as a legal basis for the processing of personal data under the GDPR. This distinction, referred to in the Guidelines, is particularly significant in clinical trials, observational studies and research activities subject to specific ethical or regulatory requirements.

In practice, indeed, withdrawal from the trial or study may give rise to uncertainties as to the possibility of continuing to store or use data already collected and lawfully processed. It is, therefore, necessary to **avoid such withdrawal being automatically interpreted as entailing, in all cases, the erasure or unusability of the data**, especially where the processing is based on legal grounds other than GDPR consent or responds to safety, pharmacovigilance, post-market surveillance *post-market* or regulatory compliance obligations.

On this point, it would, therefore, be appropriate to provide more precise indications on the effects of the withdrawal of consent and of withdrawal from participation on the processing of data already collected, clearly distinguishing the cases in which the processing is based on GDPR consent from those in which it is based on a different legal basis, such as legal obligation, public interest - as in the case of the assistance and care of patients - or legitimate interest.

2.3.2 Legitimate interest (Section 4.3)

Confindustria considers the reference to legitimate interest, under Article 6(1)(*f)* GDPR, as a suitable legal basis for processing for research purposes, including where carried out in a commercial context, to be particularly relevant.

This indication is of significant operational value for enterprises, as it clarifies that **the presence of profit-making purposes does not, in itself, preclude the possibility of considering reliance on this legal basis**. The Guidelines emphasise, indeed, that, within the balancing test, research may assume particular importance by reason of its relevance as an activity capable of producing benefits for society.

As regards the need to consider the reasonable expectations of the data subject, the recognition by the Guidelines of the fact that **they may be more or less apparent depending on the context** is shared. There are, indeed, cases in which the data subject may reasonably expect that their data will also be processed for research purposes; in such cases, this element may have a favourable bearing on the balancing test and allow a

proportionate assessment of any further safeguards that may be required. Conversely, where such expectation is less apparent, the measures provided for by Article 89 GDPR and the further safeguards apt to reduce or mitigate the impact of the processing on the rights and freedoms of data subjects take on greater importance.

It would, therefore, be important for the Guidelines to provide specific examples referring to the productive, industrial and applied context, in which, precisely by reason of the context of the collection, the relationship established with the controller and the nature of the activity carried out, the reasonable expectations of data subjects may more frequently be apparent. This may occur, for example, where the processing of data serves activities of research, development, validation, improvement or verification of products, services, processes or technologies connected with the activity of the enterprise and consistent with the existing relationship with the data subject.

2.3.3 Processing of special categories of personal data: regulatory fragmentation and applicable safeguards (Section 3.1.1, Section 4.4 and Section 4.4.3)

The Guidelines recognise that the processing of special categories of personal data for research purposes requires reliance on one of the conditions provided for by Article 9(2) GDPR, including that under point (j), and that Member States may introduce further conditions or limitations, in particular with regard to genetic, biometric or health data, pursuant to Article 9(4).

This framework, although consistent with the structure of the GDPR, gives rise in practice to significant **regulatory fragmentation** for entities operating on a European scale. Research, especially where cross-border, requires instead a sufficiently harmonised regulatory environment, capable of reducing divergences among Member States and of making the EU a competitive environment in which to invest, innovate and develop projects of strategic relevance.

The coexistence of different national rules generates legal uncertainty and application complexities, in particular in multinational projects that have a retrospective dimension and entail a re-use of data already generated and collected by individual centres (for example, in the course of providing healthcare services), as well as in multicentre clinical *trials*, in data-sharing initiatives and in the establishment of federated infrastructures, the need to coordinate legal bases, local requirements, authorisations, ethical assessments and health rules entails high costs, longer timeframes and reduced predictability.

To this is added the aspect relating to the **further safeguards** under Article 89(1) GDPR. The Guidelines state, indeed, that a controller intending to rely on one of the conditions under Article 9(2)(g), (i) or (j) may have to adopt measures additional to those imposed by law, where the processing gives rise to risks not anticipated by the legislation authorising the exemption.

While sharing the need to ensure an adequate level of protection, it is necessary to avoid this indication translating into an excessively broad burden on the controller. Where EU or Member State law authorises a given processing operation and regulates its safeguards, the related risks have already been weighed by the legislator, together with the measures deemed appropriate and specific for the rights and interests of data subjects. This is a

legislative choice, resulting from the balancing of the freedom of research and the protection of data, which the individual operator should not be called upon to reopen.

Placing on the controller the burden of assessing the insufficiency of the measures provided for by law and of supplementing them autonomously would risk creating an application uncertainty hardly compatible with the principles of legal certainty and predictability. Where the statutory safeguards prove inadequate in relation to the risks, the corrective action should fall to the legislator, through an update of the applicable framework, and not to the individual operator.

In light of these considerations, the Guidelines should promote an approach aimed at reducing regulatory fragmentation among Member States and, at the same time, at preserving legal certainty for operators.

In particular, the EDPB could promote greater convergence in application through *soft law* instruments, cooperation among supervisory authorities and co-regulation, such as a European, up-to-date and easily accessible mapping of the national rules applicable to research, with specific reference to health, genetic and biometric data; the adoption of European codes of conduct; the definition of common criteria for assessing appropriate safeguards under Article 89 GDPR; and the promotion of European data protection impact assessment (DPIA) templates for research.

It would, moreover, be appropriate to clarify that, where there is an EU or Member State legal basis authorising the processing for research purposes and regulating its safeguards, the controller is required to apply the measures provided for, without having autonomously to reopen the question of their sufficiency, save where specific and further risks linked to the concrete arrangements of the processing emerge.

2.4 Roles in the data protection chain (Section 7)

In complex research projects, the correct qualification of data protection roles is of central importance, especially where several entities are involved with contributions differing in intensity, phase and type of activity. Confindustria therefore appreciates the approach of the Guidelines according to which the qualification of roles must be carried out in functional terms, allocating responsibilities on the basis of the role actually performed by each entity, irrespective of the formal designation. This criterion is consistent with the principle of accountability under Articles 5(2) and 24 GDPR.

In this regard, the Guidelines clarify that an entity may be qualified as a controller even where it does not process personal data, processes them only to a limited extent or processes them only in pseudonymised form.

This indication, while giving weight to the substantive role performed in the processing, nonetheless requires clarification, in order to avoid uncertainties as to the obligations that can concretely be required of entities that do not have the means reasonably likely to be used to identify or re-identify data subjects.

In particular, this aspect should be coordinated with the relative notion of personal data, according to which the identifiability of the data subject must be assessed in light of the means reasonably likely to be used by the individual entity, taking into account the context

of the processing and the information actually available or accessible. This approach is confirmed by the recent case law of the Court of Justice of the European Union, according to which the qualification of pseudonymised data as personal data cannot be carried out in an abstract and undifferentiated manner, but requires verifying whether, for the entity processing them, the identification of data subjects is reasonably possible in light of the means at its disposal or to which it may reasonably have access (Court of Justice of the EU, 4 September 2025, Case C-413/23).

It follows that, where an entity has exclusively pseudonymised data and does not have access to additional information or to other means reasonably likely to be used to re-identify data subjects, the qualification of the data, of the roles and of the applicable obligations should be **assessed by reference to its concrete position, without automatic assumptions and consistently with the notion of personal data** surveillance.

It would, moreover, be useful to provide examples referring to complex research projects involving numerous partners, with contributions differing in intensity, phase and type of activity. In such contexts, indeed, the qualification of roles and the consequent identification of the applicable obligations may be particularly complex, especially where some entities are involved only in specific phases of the project, access data in pseudonymised form or have limited information in relation to the processing as a whole.

In support of this need, the Guidelines could promote *soft law* instruments, such as standard clauses or European template agreements under Article 26 GDPR, specifically designed for consortia, partnerships and research infrastructures. Such instruments would foster greater harmonisation in application, facilitate cross-border cooperation and help to reduce negotiating and organisational burdens, in particular for smaller entities.

2.5 Relationship between safeguards under Article 89 GDPR and general measures (Section 8.1)

The Guidelines distinguish the safeguards adopted under Article 89(1) GDPR from the general measures already imposed by the Regulation (Articles 5, 24, 25 and 32), recognising that a single measure may simultaneously satisfy several obligations. This is the case, for example, of access controls, which may respond both to the security requirements under Article 32 and to the safeguards required for processing carried out for research purposes.

This clarification is of significant practical relevance, as it makes it possible to avoid a merely formal layering of obligations and to give weight to the technical and organisational measures already adopted in implementation of the general principles of the GDPR, where adequately designed, documented and calibrated to the research context.

The same logic should also apply to the legitimate interest balancing *test*, when account is taken of the safeguards adopted under Article 89(1). If such safeguards were considered necessarily additional to the mandatory measures already provided for by the GDPR, there would be a risk of encouraging a disproportionate approach, inducing controllers to adopt additional measures not on the basis of the actual risks, but solely in order to strengthen their position in the balancing exercise.

It would, therefore, be appropriate to clarify that the adequacy of the safeguards must be assessed in concrete terms, in light of the nature, scope, context, purposes and risks of the processing. The safeguards under *ex* Article 89(1) should not be understood as an automatic duplication of the obligations already provided for by the GDPR, but rather as the set of measures actually suitable, according to a criterion of proportionality, to reduce or mitigate the impact of the processing on the rights and freedoms of data subjects.

It is, therefore, necessary to clarify that the measures adopted in implementation of the general principles of the GDPR may also satisfy the safeguards required by Article 89(1), where they prove concretely adequate in relation to the risks of the processing and are specifically directed at the protection of data subjects in the scientific research context, without this entailing an automatic or indiscriminate duplication of obligations.

2.6 Risk analysis and data protection impact assessment (Section 8.2)

The Guidelines identify risk analysis and, where required, the Data Protection impact assessment (DPIA)as the starting point for the adoption of appropriate safeguards under Article 89(1) GDPR, inviting controllers to consider also the possible risks to fundamental rights and freedoms other than data protection.

While sharing the need for an approach attentive to the interests of individuals, Confindustria considers that the contours of this extension should be clarified, in order to avoid uncertainties as to the scope and function of the DPIA. The latter, indeed, should **remain anchored to the assessment of the risks arising from the processing of personal data**, without turning into a general and undifferentiated assessment of every possible impact on fundamental rights.

It would, therefore, be appropriate to clarify that the DPIA coordinates with - without overlapping with - the other impact assessments that may be required by sectoral rules, such as the fundamental rights impact assessment provided for by the AI Act or the ethical assessments required in specific research fields, such as clinical trials.

In this sense, the Guidelines should promote the possibility of carrying out integrated or coordinated assessments, apt to consider the various risk profiles in a unified manner, avoiding documentary duplication and procedural overlaps , as well as single assessments for processing operations that present similar risk profiles, are carried out using the same arrangements and are protected by adequate technical and organisational measures. Such an approach would make it possible to ensure effective protection of data subjects, without disproportionately increasing the burdens on operators. Moreover, Article 35(1) of the GDPR likewise allows a single assessment to address a set of similar processing operations that present similar high risks.

In other terms, it should be clarified that the **identification of appropriate safeguards must take place according to a criterion of proportionality**, taking into account the nature, scope, context, purposes and risks of the processing, as well as the size of the controller and the complexity of the research project. This appears particularly relevant for smaller entities and for more limited research projects, for which the obligations should remain commensurate with the actual risks and the resources concretely available.

2.7 Anonymisation and pseudonymisation (Section 8.3)

The Guidelines correctly give weight to the principle of data minimisation and indicate that data should be anonymised or, where this is not feasible, pseudonymised. Pseudonymisation, where accompanied by appropriate technical and organisational safeguards, represents indeed a particularly relevant measure to reduce the risks to data subjects, while at the same time preserving the quality, usability and verifiability of the data necessary for the research.

As regards the contractual provisions that should oblige the controller that has pseudonymised the data to provide downstream the information necessary for re-identification, while understanding the protective purpose underlying this indication, it appears appropriate to clarify its scope. It is, indeed, necessary to **avoid this provision generating uncertainties as to the protective function of pseudonymisation, which is based precisely on the separation of additional information** surveillance.

It would, therefore, be necessary to clarify that any re-identification mechanisms must not frustrate the protective purpose of pseudonymisation, nor entail a generalised circulation of the additional information. Preference should instead be given to models in which it is the original controller, which holds the additional information, that enables the exercise of data subjects' rights through controlled, secure and documented procedures, without transferring such information to the entities processing the data in pseudonymised form, save to the extent strictly necessary and proportionate.

Also to be appreciated is the indication that, in order to ensure the effectiveness of anonymisation and pseudonymisation techniques, controllers should take into account the state of the art and verify their effective robustness over the course of the processing. Such verification should, however, be understood in **proportionate and risk-based terms**, avoiding it translating into a permanent and undifferentiated obligation, disconnected from the concrete evolution of re-identification risks, from the nature of the data, from the context of the processing and from the techniques used.

Lastly, in order to strengthen interpretative certainty, it would be desirable to have **constant interaction among supervisory authorities, sectoral regulatory authorities, Member State governments and European institutions** for the definition of *standards*, criteria and good practices on anonymisation and pseudonymisation in processing carried out for research purposes. Such instruments should foster a uniform and proportionate application of the rules, while at the same time ensuring the protection of data subjects, the quality of the information and the possibility of its secure and controlled circulation.