ELI
EUROPEAN
LAW
INSTITUTE

Simpler, Fairer, More Effective – Towards a Targeted Revision of EU Data Protection Law

Response of the European Law Institute

ELI

EUROPEAN
LAW
INSTITUTE

Feedback of the European Law Institute on the Digital Package – Digital Omnibus

Simpler, Fairer, More Effective – Towards a Targeted Revision of EU Data Protection law

The European Law Institute

The European Law Institute (ELI) is an independent non-profit organisation established to initiate, conduct and facilitate research, make recommendations and provide practical guidance in the field of European legal development. Building on the wealth of diverse legal traditions, its mission is the quest for better law-making in Europe and the enhancement of European legal integration. By its endeavours, ELI seeks to contribute to the formation of a more vigorous European legal community, integrating the achievements of the various legal cultures, endorsing the value of comparative knowledge, and taking a genuinely pan-European perspective. As such, its work covers all branches of the law: substantive and procedural; private and public.

ELI is committed to the principles of comprehensiveness and collaborative working, thus striving to bridge the oft-perceived gap between the different legal cultures, between public and private law, as well as between scholarship and practice. To further that commitment, it seeks to involve a diverse range of personalities, reflecting the richness of the legal traditions, legal disciplines and vocational frameworks found throughout Europe. ELI is also open to the use of different methodological approaches and to canvassing insights and perspectives from as wide an audience as possible of those who share its vision.

European Law Institute
Schottenring 16/ 175
1010 Vienna
Austria
Tel: + 43 1 4277 22101
E-mail: secretariat@europeanlawinstitute.eu
Website: www.europeanlawinstitute.eu

Approved by the ELI Council on 13.10.2025.
Final version published on 14.10.2025.

ISBN: 978-3-9505495-9-1

This publication was co-funded by the European Union's Justice Programme. Acknowledgement is also due to the University of Vienna, which has generously hosted the ELI Secretariat under successive Framework Cooperation Agreements since 2011. Views and opinions expressed are those of ELI 's only and do not necessarily reflect those of the European Union, the University of Vienna or others. Neither the European Union nor others can be held responsible for them.successive Framework Cooperation Agreements since 2011.

Supported by the European Union

Acknowledgements

Authors
Christiane Wendehorst (Professor of civil law and deputy head of the Department for Innovation and Digitalisation in Law at the University of Vienna, Austria)

Paolo Balboni (Professor of privacy, cybersecurity, and IT contract law at the European Centre on Privacy and Cybersecurity (ECPC) within the Maastricht University Faculty of Law, the Netherlands)

Jussi Mäkinen (Legal and policy expert specialising in EU data and digital regulation, Technology Industries of Finland, Helsinki, Finland)

Teresa Rodríguez de las Heras Ballell (Professor of commercial law at Universidad Carlos III de Madrid and a delegate of Spain to UNCITRAL and UNIDROIT on digital economy projects; ELI President)

Agata Szeliga (Attorney at law, partner at Sołtysiński Kawecki & Szlęzak in charge of the personal data and privacy law practice, Warsaw, Poland)

Rania Wazir (Data scientist and mathematician working on human rights-based AI technology, co-founder and CTO of leiwand.ai, Austrian delegate to international standards organisations working on AI)

ELI Project Officers
Tomasz Dudek
Marta Lages de Almeida
Margot Rebulet

Table of Contents

Executive Summary

In September 2024, the Draghi Report on the future of European competitiveness emphasised the pressing requirement for Europe to rethink its regulatory agenda, including in the context of data and emerging technologies. With regard to data protection law, the Report offers mainly two areas of criticism: First, it criticises the indiscriminate application of the General Data Protection Regulation (GDPR) to Small to medium-sized enterprises (SMEs). Second, it highlights the problem of differences among Member States in the implementation and enforcement of the GDPR as well as inconsistencies between the GDPR and other legislation in the context of AI development.

Inspired by the Draghi Report, a working group set up by the European Law Institute (ELI) has developed a range of proposals on how the GDPR could be adapted to better support the goals of competitiveness and growth. This document therefore puts forward recommendations for incorporating **targeted amendments to the GDPR within the Digital Omnibus or the broader Digital Package**.

Despite the urgent need to foster innovation and facilitate business in Europe, ELI is deeply convinced that improvements must not come at the expense of fundamental rights protection. This is why the ELI is proposing a **risk-based approach** that takes regulatory burdens off SMEs and facilitates the development and deployment of AI and other technologies, while also offering significant data protection enhancements in scenarios where citizens' fundamental rights are manifestly at risk. The aim is to create a 'win-win situation' for businesses and data subjects alike, which should enhance the protection of fundamental rights overall. This is achieved by:

- defining a **black-list of 'prohibited data processing'** operations that are so harmful that they cannot be justified even by the consent of the data subject, as well as a **white-list of 'exempted data processing'** operations that are no longer subject to the GDPR.

- introducing a **three-layered regulatory regime within the GDPR**:

  (i) an 'enhanced regime' for big, sophisticated players in the digital economy engaging in high-risk data processing;

  (ii) a 'light regime' for small, non-sophisticated players processing personal data in their day-to-day activities without engaging in high-risk processing; and

  (iii) a 'regular regime' for all other cases.

In terms of **reducing regulatory friction**, both with regard to differences between Member States and to inconsistencies between EU legal instruments in the context of AI, the ELI submits a series of proposals to facilitate the development and deployment of digital technologies in Europe. These include:

- removing uncertainties about the scope of enhanced protection under Article 9 of the GDPR;

- removing uncertainties about the legal basis for training AI and similar activities;

- proposing more targeted data subjects' rights in the context of general-purpose AI; and

- reducing differences in the implementation of the GDPR or mitigating their effects.

Furthermore, additional measures are proposed to reduce unnecessary administrative burdens, including measures in the context of engaging processors. While confining its response to the issues raised directly in the Draghi Report, the ELI also wishes to express its support for other measures, such as improved rules on cookies and other tracking technologies, as mentioned in the consultation documents.

All proposals in this document are intended to be **modular**, providing a form of 'toolbox-like' inspiration. With a few exceptions where proposed amendments are obviously interdependent, the proposals can be adopted individually or in combination, depending on political preferences.

I. Introduction

Over the past years, the European Union has taken significant steps in creating a comprehensive regulatory framework for digital technologies and ecosystems, with the goal of ensuring that technology is trustworthy, secure, and protective of fundamental rights and that there is fair competition and an environment allowing for innovation and growth. As the digital landscape rapidly evolves, the EU has recently passed several pieces of legislation that focus on data and data-driven technologies. These include, inter alia, Regulation 2016/679 (General Data Protection Regulation, GDPR), Regulation 2022/868 (Data Governance Act), Regulation 2022/1925 (Digital Markets Act), Regulation 2022/2065 (Digital Services Act), Regulation 2023/2854 (Data Act) and Regulation 2024/1689 (Artificial Intelligence Act). While these legislative initiatives have created a robust framework for the digital economy, there is a growing need for better alignment to avoid regulatory fragmentation and ensure consistency. At the same time, there is a need to identify blind spots and areas where legislation has been overtaken by technological developments, such as the mass roll-out of artificial intelligence (AI), and in particular large models of general-purpose AI.

Regulation 2016/679 has proved to be one of the most influential pieces of legislation ever adopted by the EU, raising widespread awareness of the importance of data protection and inspiring legal developments worldwide. Although it dates from 2016, its characteristic regulatory patterns, already present in Directive 95/46/EC, were developed in the 1990s or even the 1980s and have shown a high degree of resilience. However, while Regulation 2016/679 includes certain risk-based elements, recent EU legislation on digital matters has increasingly emphasised an even more risk-based approach and has focused on calibrating the regulatory requirements according to the size and resources of businesses as well as to the specific risks posed by their activities. This principle of proportionality is central to the EU's digital regulation strategy. Compared with recent EU legislation, Regulation 2016/679 takes more of a 'catch-all' approach, as it imposes relatively high regulatory burdens even on small players engaged in minimal-risk activities while not fully keeping pace with developments in terms of high-risk activities.

It is for these reasons that the ELI wishes to urge the Commission to include much more far-reaching amendments to the GDPR in the Digital Omnibus or wider Digital Package than were presented in the Omnibus IV Simplification Package in May 2025.

The suggestions submitted by the ELI below draw heavily on a tentative academic discussion draft for an 'AI Data Protection Regulation', authored by Wendehorst and published in December 2024. However, the ELI draft differs fundamentally from this earlier draft, considering feedback received from a large number of different stakeholders across Europe in 2025. It is also the product of an international, interdisciplinary working group comprising legal scholars, practising lawyers, and data scientists, and has been scrutinised and approved by the diverse constituency of jurists on the ELI Council. The most notable differences compared to the 2024 Wendehorst draft are that amendments:

- are phrased as amendments to the GDPR itself, in line with the regulatory technique of 'omnibus' legislation, in order not to further enhance the complexity of the *acquis*;
- are presented in a modular manner, enabling relevant stakeholders to select the most suitable suggestions; and
- have been radically shortened and simplified, notably by further alleviating the regulatory burden on SMEs, and are now even more closely aligned with Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (CFR).

The suggested amendments to the GDPR are presented in two batches under two headings. The first aims to make the GDPR more risk-based by introducing a three-layered regulatory regime, while the second aims to reduce friction between the GDPR and other digital economy legislation, and to facilitate innovation, particularly in the context of AI and other new technologies.

II. Lessons from the Draghi Report: A dual focus for change

In September 2024, the Draghi Report on the future of European competitiveness emphasised the pressing requirement for Europe to rethink its regulatory agenda, including in the context of data and emerging technologies. With regard to data protection law, the Report offers mainly two areas of criticism: First, it criticises the indiscriminate application of the GDPR to SMEs (Part B p 322). Second, it highlights friction created by the GDPR and other pieces of legislation in the context of AI development, warning that 'differences among Member States in the implementation and enforcement of the GDPR […], as well as overlaps and areas of potential inconsistency with the provisions of the AI Act create the risk of European companies being excluded from early AI innovations because of uncertainty of regulatory frameworks as well as higher burdens for EU researchers and innovators to develop homegrown AI' (Part B p 79, as well as Governance Chapter).

1. Taking burdens from SMEs while enhancing fundamental rights protection

Options for a more risk-based approach

Although it is widely accepted that digital economy legislation should be risk-based, creating a regulatory model that is both theoretically sound and practically straightforward remains challenging. According to the AI Act, 'risk' means the combination of the probability of an occurrence of harm and the severity of that harm, resulting in a list of prohibited AI practices and another list of high-risk AI systems. In contrast, the DSA introduces a graded system that differentiates according to the size of enterprises and imposes additional obligations on very large players based on the number of average monthly active recipients. In the context of data protection, an approach that considers both the characteristics of the actor (the data controller or processor) and the nature of the activity (the data processing itself) may be most appropriate.

Specifically, the actor-oriented dimension of risk could take into account:

- the size of the company, eg whether a controller qualifies as a micro-, small-, or medium-sized enterprise as defined in the Annex to Commission Recommendation 2003/361/EC or as a small mid-cap enterprise as defined in the Annex to Commission Recommendation 2025/1099;
- the scale of data processing, measured, in particular, by the number of individuals whose personal data is processed at any given time and further criteria, as larger-scale processing inherently increases the potential for harm, both in terms of scope and impact; and
- the extent to which a company's business model relies on data-driven activities, such as data analytics, targeted advertising, trading data, or training AI systems, reflecting that company's level of sophistication and involvement in the data economy.

On the other hand, the activity-oriented dimension of risk would focus on the specific characteristics of the data processing activity itself, including:

- the sensitivity of the information, eg whether the data includes special categories of data;
- the potential for combining data from different types and sources to generate new information, which was not originally contained in the initial datasets;
- the potential consequences for the data subject, eg whether the processing entails profiling or automated decision making that seriously affects an individual; or

- the absence of effective control, eg whether data will be disclosed to a high number of third parties.

A necessary condition: Enhancing fundamental rights protection *per saldo*

One of the main aims of the proposed regulatory framework is to reduce the regulatory burden for businesses, particularly SMEs, in areas where data processing poses a low risk to the rights and freedoms of individuals. Such a simplification would not only serve the economy but also have the potential to enhance the protection of fundamental rights by freeing up scarce resources of data protection authorities, enabling them to focus on serious cases. It would also make it easier for companies to comply, meaning that protections could be implemented more effectively.

However, the ELI is also aware that any reduction in regulatory obligations, even in low-risk scenarios, might be perceived as a weakening of data protection standards and, by extension, as a reduction in the overall level of fundamental rights protection. This concern is particularly significant given the central role that data protection plays in safeguarding the right to privacy and other fundamental rights enshrined in the CFR. The ELI firmly holds the conviction that the level of fundamental rights protection should not be lowered. On the contrary, the ELI advocates for a regulatory approach that strengthens the overall framework for data protection.

This balance can be achieved by adopting a risk-based approach that differentiates between low-risk and high-risk data processing activities. While regulatory burdens for low-risk activities can be reduced to alleviate unnecessary constraints on businesses, particularly SMEs, this should be accompanied by enhanced protections for high-risk data processing. High-risk activities – those that have the potential to cause significant harm to individuals – should be subject to stricter oversight and more robust safeguards than is currently the case. Furthermore, certain types of data processing that are deemed so harmful or invasive that they cannot be justified under any circumstances should be outright prohibited.

The idea of a three-layered regulatory regime

In order to achieve a truly risk-based regulatory framework that, *per saldo*, significantly enhances fundamental rights protection while remaining manageable, the ELI proposes a three-layered regulatory regime.

- The first layer, an 'enhanced regime', would apply to large, sophisticated players in the digital economy that engage in high-risk data processing operations; for data traders or for very large players engaging in high-risk processing with regard to a very high number of data subjects, additional obligations within the 'enhanced' regime would apply.

- The third layer, a 'light regime', is designed for small, non-sophisticated players that process personal data as part of their day-to-day activities without engaging in high-risk processing. This category would include SMEs or non-profit organisations and natural persons whose primary business activities are not data-centric.

- The second layer in between would be the 'regular regime', ie the GDPR as it stands today, and this would serve as the default framework for all other cases.

Most of the additional obligations under the enhanced regime for large players focus on consent management, particularly supporting the use of data intermediation services within the meaning of the Data Governance Act, such as personal information management services (PIMS), and enabling automated consent management by data subjects.

For SMEs, non-profit organisations and natural persons that process personal data as part of their day-to-day activities and not for commercial purposes, basically only the requirement of lawfulness of processing and the data security obligations would continue to apply. Where such actors engage in high-risk processing, they have to comply with the full set of obligations (only) for that processing.

	Large-scale controller or processor	[All parties in between]	Small-scale controller or processor
High-risk processing	enhanced	regular	regular
[Everything else]	regular	regular	light

Table: Matrix representing the three-layered regulatory regime

The idea of introducing 'red lines' as well as exemptions from the GDPR

Apart from the three layers, there should be a black-list of 'prohibited data processing' activities that are so harmful that they cannot be justified even by the consent of the data subject. This ensures that data subjects can click 'OK' without reading the terms and conditions and still trust that nothing significantly harmful will be done with their data

By way of contrast, some data processing operations pose only negligible risks to the fundamental rights of data subjects, and so should be exempt from the GDPR. This concerns the processing of personal data by a party for whom the data subject is not identifiable, a view that has now been endorsed also by the Court of Justice. It also concerns sensor data and similar data whose processing as personal data is only transitory (eg for a few seconds), and where adequate safeguards are in place to prevent any use in relation to an identifiable natural person. Furthermore, a significant proportion of business data qualifies as personal data, eg, when the business is owned by identifiable natural persons or when the data can be linked to identifiable employees, even if data is used solely with regard to the business itself. This creates unnecessary administrative burdens as well as a highly fragmented regulatory landscape, undermining the expectations associated with measures such as the Data Act, which is why enterprise and object data should be excluded from the GDPR where they are not used for a purpose associated with an identifiable natural person.

	Large-scale controller or processor	[All parties in between]	Small-scale controller or processor
Prohibited processing	X	X	X
High-risk processing	enhanced	regular	regular
[Everything else]	regular	regular	light
Exempt processing	—	—	—

Table: Matrix of regulatory regimes, integrating prohibited and exempt processing

2. Reducing regulatory friction for the benefit of innovation

Solving the 'Article 9 problem'

Special categories of personal data, as defined in Article 9 GDPR, present a particular challenge for businesses handling personal data, particularly in light of recent case law from the Court of Justice. This is why it is proposed that legal certainty be created by restricting the application of the special regime to cases where data is either inherently about sensitive characteristics or processed for a purpose related to sensitive characteristics. Additionally, further legal grounds are proposed for processing special categories of data for the fulfilment of a contract and for bias recognition and mitigation.

GDPR and AI Act: ensuring legal certainty for AI development in Europe

The GDPR, in its current form, does not align seamlessly with the unique requirements of AI. A key challenge lies in reconciling the fundamental data protection principles of data minimisation and purpose limitation with the demands of AI development and deployment. However, these principles might also possess the flexibility needed to adapt to the evolving landscape of AI technologies.

What appears to be more pressing, however, is the need to establish legal certainty in two critical areas. First, clarity is required regarding the legal basis for training AI systems on large and heterogeneous datasets. Second, the rights of data subjects, as currently interpreted, are not well-suited to address the specific challenges posed by general-purpose AI. Addressing these gaps is essential to ensure that the GDPR can effectively support the responsible development and use of AI while safeguarding individual rights.

Reducing differences in implementation or enforcement

As highlighted in the Draghi Report, the varying implementation and enforcement of the GDPR across Member States pose significant challenges for companies operating in multiple jurisdictions or collaborating with partners in other Member States. One notable example cited in the Report is the divergence in national approaches regarding age thresholds for minors' consent; other examples include data protection in scientific research and the employment context. To address these challenges, the ELI proposes the introduction of a much-needed conflict-of-laws provision. This provision would ensure that a controller engaged in cross-border data processing can normally rely on the data protection laws of their home country and that, in cases involving multiple controllers, the parties would have the option to agree on the applicable data protection law, while also imposing safeguards against 'data protection forum shopping'.

In addition, the ELI recommends reducing fragmentation in the practices of supervisory authorities and centralising the supervision of the largest players in the data economy at the Union level. It also recommends providing a harmonised list of the kind of processing operations which are subject to the requirement for a data protection impact assessment or for which no data protection impact assessment is required, which is valid throughout the Union, as well as a harmonised illustrative list of legitimate interests within the meaning of Article 6(1)(f) of the GDPR.

III. Modular proposals for a truly risk-based approach

1. Lists of prohibited and exempt processing operations

Prohibiting very harmful data processing activities

After Article 6 of Regulation 2016/679, the following Article 6a is inserted:

Article 6a

Prohibited data activities

1. The following processing operations and other activities shall be prohibited in any case and cannot be based on the consent of the data subject or any other legal ground referred to in Article 6:

a. inducing a data subject or other controller or processor to generate or disclose personal data, or consent to, or otherwise trigger the generation or disclosure of, personal data, through misleading or aggressive practices or using subliminal techniques, including by way of dark patterns;

b. processing of personal data by a controller on the basis of the data subject's purported consent, even though the controller knows, or can reasonably be expected to know, that the data subject or a third party is likely to suffer significant harm as a result and the controller cannot reasonably assume that the data subject would have given consent if the data subject had foreseen this risk;

c. transferring personal data to a third party or promoting or substantially facilitating the processing of personal data by a third party despite the fact that the controller or processor knows or can reasonably be expected to know that the third party will materially breach its obligations to the data subject by such processing in a way likely to cause significant harm to the data subject;

d. providing a product or service to a controller or processor despite the fact that the provider of the product or service knows, or can reasonably be expected to know, that, because of the design of the product or service, the controller or processor will materially breach its data-related obligations to the data subject when using the product or service.

2. The prohibitions in this Article are subject to generally recognised grounds of justification, including that a party is required by law to engage in the prohibited data activity, without any relevant margin of discretion.

3. The prohibitions in this Article are without prejudice to any prohibitions following from other Union law or national law adopted in accordance with Union law, including the law of tort, anti-discrimination law, consumer protection law and competition law.

Proposed accompanying recitals:

Certain harmful data activities should be explicitly prohibited, so that they cannot be justified by any of the legal grounds listed in Article 6, notably not by the consent of the data subject. Data subjects should be able to rely on the fact that, even if they click 'OK' without reading and understanding the terms, nothing significantly harmful will happen. This would put data subjects in a position similar to that afforded

to them by consumer contract law under Directive 93/13/EEC (Unfair Contract Terms Directive). It should be emphasised that this does not affect the possible application of national law implementing Directive 93/13/EEC to pre-formulated consent forms that are not negotiated individually.

Like Article 5 of Regulation 2024/1689, which sets out a list of prohibited AI practices, Article 6a of Regulation 2016/679 therefore sets out a list of prohibited data activities. These are data activities that are generally unacceptable because they are incompatible with fundamental principles of fairness enshrined in Union and Member State law and may cause significant harm to data subjects. They can be seen as a basic list of 'data torts', compensating for the fact that tort law in many Member States is not well equipped to deal with data-related situations. Many of them were inspired by the 'Principles for a Data Economy' by the American Law Institute and the European Law Institute ('ALI-ELI Principles'). Much like tort law, they are necessarily open-ended in order to cover a wide range of situations. The prohibitions are without prejudice to the fact that, in many situations covered by the prohibitions, the processing of personal data may already take place without a legal basis under Regulation 2016/679. The list of prohibited data activities serves as a safety net to fill gaps that may arise, for example where processing could potentially be based on the data subject's consent under Regulation 2016/679 and Directive 2002/58/EC (ePrivacy Directive), or in situations where Regulation 2016/679 is inapplicable.

A key case of a prohibited data activity is inducing a data subject or other controller or processor to generate or disclose personal data, or consent to, or otherwise trigger, the generation or disclosure of personal data, through misleading or aggressive practices or using subliminal techniques, including by way of dark patterns.

Another key case is the processing of personal data on the basis of the data subject's consent, where the processing is highly likely to cause significant harm to the data subject or a third party and the controller cannot reasonably believe that the data subject would have consented if aware of this risk. This case can cover a wide range of different practices. While Regulation 2016/679 lays down rather strict requirements for consent to be valid, such as that consent must be freely given, specific, informed and unambiguous, there is still the possibility that data subjects may not read or understand the information given to them, or that they may underestimate the risk associated with purposes such as price personalisation. For a practice to qualify as a prohibited data activity that triggers the relevant sanctions under Regulation 2016/679, it must cause significant material or immaterial harm to the data subject, and the controller must know this, or the situation must be such that the controller can reasonably be expected to know this. The harm must be inflicted by the controller or, where inflicted by a third party, this must be foreseeable for the controller. For the harm to be significant, it must be objectively ascertainable and go well beyond mere subjective feelings of discomfort. An example would be relying on the data subject's consent to use very private or even intimate social media data in the context of recruitment, which foreseeably reduces the data subject's chances of success in their professional career. In addition, the harm must be such that the data controller could not reasonably believe that the data subject would have given consent. For example, the provider of social media services cannot reasonably assume that the data subject, by consenting to the use of very private data for 'contractual offers by third parties', had ever anticipated the use in a recruitment situation. Likewise, if the data subject has consented to the processing of personal data for the purpose of 'personalising offers', there is no reason to believe that the data subject would have consented if they had anticipated that they would pay an average of 10% more.

Obviously, it is a prohibited data activity to process personal data where the controller itself would be in breach of contractual or statutory obligations, for example obligations under a confidentiality agreement or professional secrecy. However, it is also a prohibited practice to make personal data available to a third party, or to encourage or substantially facilitate the processing of personal data by a third party, when the controller knows, or can reasonably be expected to know, that the third party will materially breach its obligations to the data subject by such processing. This makes up for the lack of explicit due diligence obligations in Regulation 2016/679 when personal data is disclosed to another controller rather than to a processor. For example, if a hospital has obtained the data subject's explicit consent to use data for certain research purposes and to share

the data with relevant research institutions, sharing the data for such purposes would still be a prohibited data activity if the hospital has reason to believe that a particular research institution will not apply any data security measures and thus data subjects are likely to suffer harm.

A closely related prohibition is that of providing a product or service to a controller or processor where the provider knows, or can reasonably be expected to know, that, because of the design of the product or service, the controller or processor will materially breach its data-related obligations to the data subject when using the product or service. An example is where a provider of software solutions used in school education designs the software in such a way that schools, if they want to use the functionalities of the software, are forced to act in violation of Regulation 2016/679 (eg because the only possible legal basis for processing students' personal data in the individual situation would be consent, but consent obtained from students or their parents would not be considered 'free'). If the school qualifies as a small-scale controller and benefits from the exemption under Article 2a, this exemption must not benefit third parties in the context of prohibited data activities. For example, if a third party provides digital services to the school that qualifies as a small-scale controller and forces that school to collect data from its students or employees in a way that would be in breach of Regulation 2016/679 if Regulation 2016/679 fully applied to the SME, the third party should not be allowed to argue that there is no prohibited data activity because the SME was not required to comply fully with Regulation 2016/679.

Some of the prohibitions may need to be interpreted narrowly where a party processing personal data has acted on the basis of legitimate interests protected by other laws, such as the law on freedom of information and expression, or for purposes such as fraud detection. The prohibitions are also subject to generally recognised grounds of justification, including that a party is required by law (eg because of a court judgment) to engage in the prohibited data activity, without any relevant margin of discretion. Conversely, obligations arising from other legislation may also be disregarded if fulfilling them would constitute a prohibited data activity. For instance, if a user of a connected product or related service requests that a data holder make personal data available to a data recipient under Regulation 2023/2854, and the data holder is presented with proof of the data subjects' consent but knows that it has been obtained through fraud or misleading practices, the data holder should not share the data with the recipient, as this would constitute a prohibited data activity.

The prohibitions are without prejudice to prohibitions deriving from other Union or national law, including tort law, anti-discrimination law, consumer protection law and competition law. The difference is that if a data activity falls under one of the prohibitions in the list, it will trigger the sanctions provided for in Regulation 2016/679. Where prohibitions overlap with prohibitions set out elsewhere, an activity may trigger the sanctions provided for under Regulation 2016/679 as well as the sanctions imposed under other law. For example, the prohibition of inducing a data subject to disclose personal data through misleading or aggressive practices or the use of subliminal techniques, including through any dark patterns, will often already be prohibited under Directive 2005/29/EC or Regulation 2024/1689. As mentioned above, contractual terms that are not individually negotiated and that relate to the processing of personal data will often be considered unfair under Directive 93/13/EEC and possibly Regulation 2023/2854.

Exempting minimal-risk processing of personal data

After Article 2a of Regulation 2016/679, the following Articles 2b and 2c are inserted:

Article 2b

Relative anonymisation and non-personal use of personal data

1. This Regulation shall not apply to the processing of personal data by a party who, for technical and/or organisational reasons, is unable to identify the data subject by any means reasonably likely to be used.

2. This Regulation shall not apply to the processing of personal data where:

a. the processing is merely transitory in nature; and

b. the processing is for a purpose that is unrelated to a data subject as an identified or identifiable natural person; and

c. appropriate technical and/or organisational safeguards are in place to prevent any use of the data for a purpose related to the data subject as an identified or identifiable natural person up to the point when the data are irreversibly anonymised or erased.

3. This Regulation shall not apply to the processing of personal data where:

a. the data relate primarily to an entity other than a natural person, such as an enterprise or an object, and the data subject is associated with that entity exclusively as owner, legal representative, point of contact, person handling the object, or in a similar function; and

b. processing of the data is for a purpose that is not specifically related to the data subject in a personal capacity.

Proposed accompanying recitals:

In Case C-413/23 P – *EDPS v SRB*, the Court of Justice held that pseudonymised data must not be regarded as constituting, in all cases and for every person, personal data for the purposes of the application of Regulation 2018/1725, and the same should hold true for Regulation 2016/679. According to the Court, pseudonymisation may, depending on the circumstances of the case, effectively prevent persons other than the controller from identifying the data subject in such a way that, for them, the data subject is not, or is no longer, identifiable. For example, where pseudonymised data are transferred to a processor and that processor cannot identify the data subjects, processing by that processor is not subject to Regulation 2016/679. However, the Court also held in that decision that the data remained personal data for the controller, which is why the controller remains under an obligation to inform the data subjects prior to the transfer of the data at issue and irrespective of whether or not that data were personal data, from the processor's point of view, after any potential pseudonymisation. Article 2b(1) codifies this judgment by stating that Regulation 2016/679 does not apply to the processing of personal data by a party who, for technical and/or organisational reasons, is unable to identify the data subject by any means reasonably likely to be used.

In our modern, data-driven world, large amounts of data are constantly collected by sensors and are either deleted soon after or within the device to which the sensor belongs, or are irreversibly anonymised during transmission to the collecting entity. During a very short period of time, the data may be considered personal data, either because the data subject is close to the sensor and can therefore still be identified, or because the information contained in the data is in itself linked to the data subject as an identified or identifiable natural person. This creates unnecessary uncertainty and regulatory burdens even in cases where the legitimate interests of the data subjects are not at risk. This is in particular the case where the processing of personal data is transitory (eg only for a few seconds or minutes) and for a purpose which is not related to the data subject as an identified or identifiable natural person (eg because all that matters is whether there is a person in front of the sensor or not). For processing to be considered only a minimal risk, however, it is also a requirement that appropriate technical and/or organisational safeguards are in place to prevent any use of the data for a purpose related to the data subject as an identified or identifiable natural person. Such safeguards could, for example, consist in the automatic and irreversible anonymisation of the data, which takes place before anyone could possibly use the data for a purpose related to an identified or identifiable natural person. By contrast, where data are temporarily stored with a view to their possible association with an identified or identifiable natural person, as may be the case, for example, with video surveillance in publicly accessible places, Regulation 2016/679 and possibly other relevant legislation, such as Regulation 2024/1689 or Directive 2016/68, shall continue to apply.

Much of the recent legislation, not least Regulation 2023/2854, deals with the sharing and re-use of non-personal data, which is primarily business data that relates to an enterprise, or to a connected product, but not to a natural person. Strictly speaking,

however, much of this data will also qualify as personal data under Regulation 2016/679, simply because it can be linked to a natural person owning a business or product or a natural person operating a machine, such as a particular employee working a particular shift on the production line, or a particular driver driving a company van. If data protection law had to be complied with in all these situations, there would be little scope for legislation promoting the sharing and re-use of non-personal data. In addition, the requirement to comply with data protection laws because business partners become aware of some employees' names and contact details, eg because they serve as point of contact for a particular transaction, has created a significant administrative burden despite there being no specific need for protection. Therefore, such data should not be considered as personal data, as long as the processing is not carried out for a purpose relating to the natural persons concerned (eg the particular worker or driver) in a personal capacity. For example, if a farmer shares agricultural data with the manufacturer of a smart tractor, the agricultural data primarily relate to the farm and the soil and not to the farmer as an individual natural person. However, Regulation 2016/679 would fully apply if the agricultural data were used, for example, to assess the skills and personality of the individual farmer, or to make personalised offers to that farmer based on their personal data. It should be noted that this does not affect in any way the application of Directive 2002/58/EC to subscribers who are not natural persons.

2. Taking regulatory burdens from SMEs and shifting them to those who can shoulder them

The concept of 'small-scale controllers' and 'small-scale processors'

After point 8a of Article 4 of Regulation 2016/679, the following point 8b is inserted:

8b. 'small-scale controller' or 'small-scale processor' means a micro, small- or medium-sized enterprise as defined in Commission Recommendation 2003/361/EC, a not-for-profit organisation or an individual:

a. that does not qualify as a large-scale controller or large-scale processor within the meaning of point 8a; and

b. for which the processing of personal data, including through targeting of commercial communications, personal data analytics, refining personal data, trading personal data, or the development, placing on the market or putting into service of artificial intelligence that has been trained with personal data, is not a core business activity.

Public authorities do not qualify as small-scale controllers or processors where they act in performance of sovereign powers.

The Commission is empowered to adopt delegated acts to supplement this Regulation by specifying the methodology for determining whether the processing of personal data is a core business activity, including by defining quantitative thresholds;

Proposed accompanying recitals:

A 'small-scale controller' or 'small-scale processor' refers to a micro-, small-, or medium-sized enterprise as defined in Commission Recommendation 2003/361/EC, a not-for-profit organisation, or an individual that does not qualify as a large-scale controller or processor and for which processing of personal data is not a core business activity, with 'business' being understood in a broad sense and comprising, in the case of a non-profit organisation, any core activity of the organisation. This normally means that the controller or processor does not generate any significant revenue through activities such as processing personal data on behalf of others, trading data, targeting commercial communications, data analytics, or developing or placing on the market or putting into service artificial intelligence. Where a party earns money by processing personal data on behalf of others, this should be considered as revenue specifically from the processing of personal data only where the data-related aspect of the activity is dominant, which is not the case, for example, where the processing of personal data is only a necessary step for providing entirely different services, such as accounting or payroll services. In the case of a non-profit organisation that depends on fundraising, simply

managing the data of donors, such as for bookkeeping or accounting purposes or for issuing tax certificates is not a core business activity as it is merely ancillary to the fundraising itself. However, where a non-profit organisation engages in sophisticated targeting of potential donors, processing personal data may become a core 'business' activity of that organisation. The Commission shall adopt delegated acts to further define the methodology for determining whether the processing of personal data is a core business activity, including by defining quantitative thresholds. If a small-scale controller or processor grows or becomes more active in the data economy and exceeds the thresholds, it will lose the privileges associated with its small-scale controller or processor status, with future effect.

The concept of 'small-scale controller' or 'small-scale processor' does not include public authorities that process personal data in the performance of sovereign powers. Therefore, the exemptions under Article 2a cannot be relied on, for example, by authorities involved in taxation or issuance of building permits. However, a school, research institution or public transport system operated by a municipality, for example, could benefit from the exemption as these are tasks that could as well be provided by private economic operators.

A 'light regime' for other than high-risk data processing

After Article 2 of Regulation 2016/679, the following Article 2a is inserted:

Article 2a

Exemptions for small-scale controllers and processors

1. As far as small-scale controllers and processors process personal data without engaging in high-risk data processing, only the following provisions of this Regulation, in addition to the general provisions in Chapter I, shall apply:

a. Article 6 on lawfulness of processing and Article 6a on prohibited data activities;

b. Articles 28 and 29 on the obligations of processors; and

c. Articles 32 to 34 on security of processing

all of which shall be implemented and enforced through other laws within the meaning of paragraph 2. Small-scale controllers and processors shall, by appropriate means and in a transparent manner, inform data subjects of the fact that they rely on the exemption under this Article.

2. Member States shall ensure that small-scale controllers and processors remain subject to obligations following from laws other than data protection law, including laws protecting private and family life and the laws of employment, unfair competition, contract, or tort. Such other law must be interpreted and applied in a way that ensures conformity with Articles 7 and 8 of the Charter, including by ensuring the right to access data which has been collected concerning a data subject, and the right to have it rectified.

3. The full application of this Regulation to third parties that receive personal data from the small-scale controller or processor shall remain unaffected. The first controller in the chain that is not exempted under paragraph 1 shall be responsible for fulfilling the obligations of a controller, including providing information in accordance with Articles 13 and 14 and complying with the data subjects' rights.

A contractual provision unilaterally imposed on a small-scale controller by a third party that is likely to undermine the exemption in paragraph 1, such as by shifting to the small-scale controller or processor the administrative burdens associated with the performance of a controller's obligations, shall not be binding on the small-scale controller, except to the extent absolutely necessary to protect the rights and legitimate interests of data subjects.

Proposed accompanying recitals:

Data protection law is a highly complex area of law. In the 1990s or earlier, when the regulatory patterns of Regulation 2016/679 were developed, only very

few units within an enterprise were involved in the systematic processing of personal data in filing systems (eg the units in charge of employee files, accounting and billing, or a customer database), and not all of them used automated data processing. Small and micro-enterprises or natural persons pursuing a business, craft or profession were often not even close to the scope of data protection law. This has changed fundamentally as each individual uses multiple electronic devices, is connected to the rest of the world via the Internet, and constantly generates, stores and transmits vast amounts of data, most of which can be classified as personal data. Given the ubiquity of data processing activities, it has become increasingly difficult to strictly comply with Regulation 2016/679 in all respects, especially as most data processing activities pose no, or only minimal, risk to the fundamental rights of natural persons. This situation may lead to a feeling that strict compliance with Regulation 2016/679 is not of the essence, potentially undermining the rule of law and democracy. At the same time, we have often seen the limited resources of data protection authorities being used up by minor cases that would normally be dealt with effectively in other areas of law, such as disputes between landlords and tenants or between employers and employees, leaving insufficient resources for the major cases that go to the heart of data protection as a fundamental right.

For these reasons, small-scale controllers and processors should be exempted from the application of most provisions of Regulation 2016/679 to the extent that their data processing does not involve (prohibited or) high-risk data processing within the meaning of point 2a of Article 4. This means that, for example, the owner of a small hotel that collects personal data from guests only for purposes such as billing and accounting or to comply with applicable public law requirements, would no longer have to provide its guests with lengthy data protection notices or worry about other requirements under Regulation 2016/679. The hotel owner would only need to ensure that it processes personal data lawfully and without engaging in any prohibited data activities. The same would apply to a small university that processes student data only for purposes such as enrolment, grading and awarding of academic degrees, without, for example, engaging in student profiling. However, there are certain obligations from which small-scale controllers and processors cannot be exempted. This concerns, first of all, appropriate data security measures. Regardless of its size, a small-scale controller or processor must take appropriate technical and organisational measures to ensure a level of data security appropriate, in particular, to the risk of unauthorised disclosure of or access to personal data. Where a data breach occurs, even a small-scale controller and processor may be under an obligation to notify data subjects, eg so that they can take appropriate steps to protect themselves against harm. The same applies to the obligations of a small-scale processor under Articles 28 and 29 of Regulation 2016/679. However, the implementation and enforcement of these applicable provisions occurs through general laws other than data protection law, such as contract or tort law.

The fact that small-scale controllers or processors are exempted from the application of most provisions of Regulation 2016/679 as far as they do not engage in high-risk data activities does not mean that they can handle personal data at their own discretion. Apart from the prohibitions in Article 6a, the obligations of data processors and the requirement to maintain an adequate level of data security, they are subject to general laws, including laws protecting private and family life and laws relating to employment, unfair competition, contract or tort. One of the main considerations underlying the exemption from data protection law is to ensure that minor cases involving parties that are less sophisticated in terms of personal data management should be governed by very general laws. A wide range of service providers have to comply with professional secrecy rules, which already provide a robust framework to protect the rights and legitimate interests of the data subject. Employers are bound by labour law, which will include provisions to protect employees from disproportionate surveillance. Other parties will be bound by contractual or pre-contractual obligations, including the implied obligation not to infringe the rights and legitimate interests of the other party, the breach of which will give rise to a claim for damages. Finally, parties may be liable in tort or under the law of unfair commercial practices for particular damage they cause to others.

It is essential that the interpretation and application of such other laws ensure compliance, in particular, with Articles 7 and 8 CFR. Article 8 CFR provides that everyone has the right to the protection of

personal data concerning them and that such data must be processed fairly for specified purposes and on a legitimate basis laid down by law. In addition, everyone has the right of access to data collected about them and the right to have it rectified. For example, if a company qualifying as a small-scale controller were to deliberately start collecting its customers' personal data in an indiscriminate manner, without any good reason and far beyond what is covered by any legal basis, simply for the sake of power or with a view to possibly selling the data later, this would have to be qualified as a breach of contract and possibly as a tort under the applicable national law. Similarly, if an employee suspected that their personnel file contained erroneous references to an alleged mental illness, national employment, contract and/or tort law would have to be interpreted to mean that the employee had a right to access their file and have the information corrected.

As the extent to which general laws are adequate to deal appropriately with situations involving personal data may vary from jurisdiction to jurisdiction, it is also essential that Member States accept personal data and digital phenomena as part of our modern reality and do not consider them as something outside the scope of their general laws that can safely be ignored and left to Union digital legislation. That is why Article 2a includes an obligation for Member States to ensure that their laws are interpreted and applied in a way that recognises the importance of privacy and data protection and in a manner that is appropriate to the nature of the personal data, eg by interpreting and applying national law in the light of the principles laid down in Article 5 of Regulation 2016/679. This means, for example, that a Member State should not be allowed to deny a data subject a claim under tort law on the sole ground that the damage was caused by the misuse of personal data. On the other hand, Member States should not be allowed to undermine the aim of Article 2a to remove regulatory burdens by simply continuing to apply the provisions of Regulation 2016/679 and Directive 2002/58/EC (as national law) to small-scale controllers and processors. This is why Article 2a also provides that Member States should interpret and apply their laws in a way that respects the exception in Article 2a(1).

Where a small-scale controller or processor is largely exempted from the scope of Regulation 2016/679 or Directive 2002/58/EC by virtue of Article 2a, this should not benefit third parties, such as parties that have received data from the small-scale controller or processor. Where such third parties do not themselves qualify as small-scale controllers or processors, they remain bound by Regulation 2016/679 or Directive 2002/58/EC and have to fulfil all obligations of a controller or processor. The first controller in the chain that is not exempt from a controller's obligations shall be responsible for fulfilling a controller's obligations, including the information obligations, under Regulation 2016/679. This means, in effect, that the burden of consent management (where consent is the relevant legal basis) rests on the first controller in the chain that is not exempt from Regulation 2016/679 or Directive 2002/58/EC by virtue of Article 2a.

A contractual provision which is unilaterally imposed on a small-scale controller and which is likely to undermine the exemption will normally not be binding on the small-scale controller. This would be the case, for example, with an obligation to resume consent management on behalf of parties responsible under the first subparagraph of paragraph 3, thereby shifting the administrative burden of fulfilling the controller's obligations to the small-scale controller as if there were no exemption. To some extent, this may be necessary to protect the rights and legitimate interests of data subjects, eg where another party would otherwise need to obtain the contact details of data subjects in order to provide information to them because complying with the obligations under Regulation 2016/679 in other ways is technically impossible. In such exceptional cases, a small-scale controller may, by exception, be entrusted with consent management and similar tasks under a contractual agreement with the party that would otherwise bear this responsibility. However, even in this exceptional scenario, the other party must take all reasonable steps to provide maximum support to the small-scale controller or processor.

Fewer administrative burdens in the context of engaging data processors

Article 28(3), first sub-paragraph of Regulation 2016/679 shall be replaced by the following:

3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law that is binding on the processor with regard to the controller. Without prejudice to any more specific or more far-reaching provisions in that contract or other legal act, the processor: ….

In Article 28(4), the words: 'the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3' shall be replaced by the words: 'the sub-processor shall be subject to the obligations under paragraph 3. Where the contract or other legal act between the controller and the processor sets out additional data protection obligations, the same obligations'.

Proposed accompanying recital:

Processors are currently subject to specific obligations under Articles 28 and 29 of Regulation 2016/679. Many of these obligations are imposed on processors by law, but some have so far been subject to an obligation to enter into a contract between the controller and the processor. Regulation 2016/679 is based on the generalised assumption that in the relationship between the controller and the processor, the controller is in the driving seat because, by definition, the controller determines the purposes and means of the processing. While this generalised assumption may be true in a number of cases, it does not correspond to the commercial reality in many situations where the processor is in a much better bargaining position and can unilaterally determine a package of means, and sometimes purposes, which the controller can only accept or not on a 'take it or leave it' basis. In practice, the requirement of having to negotiate a contract that is in conformity with Article 28 has created an unnecessary administrative burden for controllers, particularly small-scale ones and others with a comparatively weak bargaining position. In addition, as the parties were not permitted to deviate from the requirements in their contract in any way that would reduce or dilute the obligations set out in Article 28, the contractual obligation was entirely superfluous. This is why the obligations should lie with processors under the law. Needless to say, parties are free to include other details or negotiate provisions that improve data subject protection through party autonomy.

3. Enhancing fundamental rights protection against high-risk data processing

The concept of 'large-scale controller' and 'large-scale processor'

After point 8 of Article 4 of Regulation 2016/679, the following point 8a is inserted:

8a. 'large-scale controller' or 'large-scale processor' means a controller or a processor that:

a. has been designated as a gatekeeper pursuant to Article 3 of Regulation 2022/1925; or

b. processes, at any point during a calendar year, personal data of over (100,000) data subjects in the Union, not including:

i. the controller's or processor's employees; and

ii. natural persons whose personal data are processed exclusively as far as this is necessary for the performance of a contract to which these persons are party, or otherwise clearly requested by these persons, or necessary for compliance with a legal obligation to which the controller or processor is subject.

A party shall not be able to avoid qualifying as a 'large-scale controller' or 'large-scale processor' by artificially dividing its activities among several of its subsidiaries, conducting some activities through parties qualifying as joint controllers within the meaning of Article 26 or by not carrying out the activities in question through a separate legal entity. The Commission is empowered to adopt delegated acts to supplement this Regulation by specifying the methodology for determining whether the quantitative threshold is met;

Proposed accompanying recital:

In line with the risk-based approach, new definitions include those referring to controllers or processors of different size and significance. A 'large-scale controller' or 'large-scale processor' refers to a controller or processor that has either been designated as a gatekeeper under Article 3 of Regulation 2022/1925 or processes the personal data of more than (100,000) data subjects at any point during a calendar year. However, in order not to capture companies that are not active in the data economy, this should exclude employees as well as natural persons whose personal data are processed exclusively as far as this is necessary for the performance of a contract to which these persons are party, or otherwise clearly requested by these persons, or necessary for compliance with a legal obligation to which the controller is subject. For example, a large machinery manufacturer that employs 150,000 people and processes their personal data exclusively in their capacity as employees does not qualify as a large-scale controller, unless it engages in other significant data-related business activities. This would not change if the same manufacturer paid for advertising services and the provider of those services engaged in personalised advertising using personal data, but the advertising service provider would likely qualify as a large-scale controller. Similarly, an electronics shop that processes the personal data of 200,000 customers exclusively for billing, accounting or commercial guarantee purposes would not qualify as a large-scale controller. However, if the electronics shop were to start sending targeted commercial communications for purposes other than fulfilling a contract or otherwise at the clear request of the data subjects, it would qualify as a large-scale controller. In order to avoid circumvention of Regulation 2016/679, a controller or processor cannot avoid being classified as a 'large-scale controller' or 'large-scale processor' by artificially dividing its activities among subsidiaries, delegating tasks to other parties acting as joint controllers, or operating through separate legal entities. The Commission is empowered to adopt delegated acts to further define the methodology for determining whether this quantitative threshold is met. This also applies to the point in time at which a controller or processor becomes a 'large-scale controller' or 'large-scale processor' if the threshold is exceeded during a calendar year.

A harmonised list of 'high-risk data processing' operations

After point 2 of Article 4 of Regulation 2016/679, the following point 2a is inserted:

2a. 'high-risk data processing' means the processing operations listed in Annex I that pose a high risk to the interests or fundamental rights and freedoms of data subjects; the Commission is empowered to adopt delegated acts to amend Annex I by adding, deleting or modifying use-cases of high-risk data processing operations, after having consulted the Board referred to in Article 68;

The following Annex I is added to Regulation 2016/679:

ANNEX I

High-risk data processing within the meaning of point 2a of Article 4 means any of the following:

a. trading personal data;

b. profiling of natural persons, unless this is necessary for the performance of a contract to which the data subject is party or otherwise clearly requested by the data subject, or necessary for compliance with a legal obligation to which the controller is subject;

c. processing of personal data with a view to subjecting a natural person to a decision based solely on automated processing which produces legal effects concerning that person or similarly significantly affects that person;

d. processing of any biometric data, genetic data or personal data resulting from direct measurement of body functions, such as heartbeat, pulse or brain activities;

e. processing of personal data to record or infer sensitive characteristics or apply any differential treatment based on sensitive characteristics, except as far as this is necessary for compliance with a legal

obligation following from employment or social security law to which the controller is subject;

f. systematic monitoring of a publicly accessible physical or virtual space;

g. transferring personal data to third countries based on Article 49(1)(a) to (d).

In the interest of simplification of the wording of the above and other proposals made in this document, some further definitions should be added:

After points 4 and 15 of Article 4 of Regulation 2016/679, the following points 4a and 15a are inserted:

4a. 'trading' personal data means making personal data available to other controllers in return for payment, in cash or in kind, without effective means of ensuring that the other controllers comply with their obligations towards data subjects, unless this is necessary for the performance of a contract to which the data subject is party or otherwise clearly requested by the data subject or necessary for compliance with a legal obligation to which the controller is subject;

15a. 'sensitive characteristics' means racial or ethnic origin, migration status, political opinions, religious or philosophical beliefs, disability, state of health, the emotional or psychological state, trade union membership, a person's sex life or sexual orientation, and criminal convictions;

Proposed accompanying recitals:

Similar to Article 6 and Annex III of Regulation 2024/1689, which set out a list of high-risk AI practices, point 2a of Article 4 and Annex I of Regulation 2016/679 set out a list of high-risk data processing operations. The list has a triple role. First, having a uniform list of high-risk processing operations helps reduce fragmentation and uncertainty in the context of Article 35 of Regulation 2016/679. Second, engaging in high-risk data processing operations triggers specific obligations for large-scale controllers under Article 8a and, if performed by data traders or on a very large scale, also additional obligations under Articles 39a and/or Article 39b. Third, as far as small-scale controllers engage in high-risk processing operations they do not enjoy the privilege under Article 2a but remain subject to the regular regime of Regulation 2016/679. Most of the cases of high-risk processing listed are already subject to more stringent requirements under Regulation 2016/679 and other law. In order to make the system future-proof, the Commission is empowered to adopt delegated acts to amend Annex I by adding or modifying use-cases of high-risk data processing operations

One of the high-risk processing operations is trading personal data. Making personal data available to other controllers is generally an activity that puts the rights of the data subject at risk, in particular where there are no effective means of ensuring that the other controllers comply with their obligations vis-à-vis the data subject. The situation is particularly critical where data are made available in return for payment in money or other consideration, ie where personal data are 'sold' to others. Even in cases where such activities are compliant with Regulation 2016/679 (eg because they are covered by the data subject's consent), they should at least be considered as high-risk data processing operations. The data does not have to be actively transferred to other controllers, but it would be sufficient to allow other controllers to collect data, for example by allowing them to track visitors to a website operated by the first controller. Likewise, the concept of trading personal data encompasses direct transactions, such as selling datasets, as well as indirect arrangements, such as granting access to personal data or usage rights in exchange for commercial gain, partnership opportunities or reciprocal data-sharing agreements. Such sharing of personal data should not qualify as a high-risk data activity, though, if it is necessary for the performance of a contract to which the data subject is party or otherwise clearly requested by the data subject (in particular for entering into pre-contractual negotiations at the request of the data subject), or necessary for compliance with a legal obligation to which the controller is subject. This includes, for example, the situation where data holders make data available to a data recipient in compliance with their obligations under Article 5 of Regulation 2023/2854.

Another type of high-risk processing is the profiling of natural persons, at least unless this is necessary for the performance of a contract to which the data subject is

party or in order to take steps at the request of the data subject prior to entering into a contract or otherwise clearly requested by the data subject. 'Profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict certain aspects concerning that natural person, as defined in Article 4(4) of Regulation 2016/679. To be considered as profiling, the purpose of the automated processing must involve some form of qualified evaluation, assessment or prediction. For example, if a university collects the grades that a student has received in different classes in order to determine whether the student qualifies for an academic grade, this may amount to an assessment, but the assessment is not made by means of a qualified operation transforming input data into a non-equivalent entity as output data, and, besides, such processing of personal data is clearly necessary for the performance of the education contract. However, if the same university collects a range of student data in order to predict the likelihood of early dropout for individual students (eg in order to offer them additional training), this goes beyond a simple mathematical operation and constitutes profiling that is, according to the strict test applied by the Court of Justice (C-252/21 and others), not necessary for the performance of the education contract. Similarly, if a company sends each customer who has bought a particular product from that company an offer for maintenance services related to that product, this may involve a prediction that those customers may need the services. This prediction, though, is not made by means of combining different types of data, but simply by matching product and related service and should not qualify as profiling. By contrast, if the same company analyses its customers' consumption patterns in order to provide them with highly personalised offers, this should be considered profiling, and it is not required for the performance of a contract (it could theoretically have been 'clearly requested' by the data subject, but 'request' is definitely much more than 'consent' and will usually not be made in such a situation).

A similar high-risk activity is the processing of personal data with a view to subjecting a natural person to a decision based solely on automated processing which produces legal effects concerning that person or similarly significantly affects that person, whether or not this involves profiling. This should be understood in line with the corresponding provision in Article 22 of Regulation 2016/679.

Another high-risk data activity is the processing of any biometric data, genetic data or data generated by the direct measurement of body functions. 'Biometric data' should be understood in line with Article 3 point 34 of Regulation 2024/1689 and means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, whether or not they allow or confirm the unique identification of that person. It should be stressed that biometric data are only such data as have undergone specific processing and do not include, eg, a simple photograph, even if that photograph would allow the unique identification of a person. By contrast, where data result from direct measurement of body functions, such as heartbeat, pulse or brain activities, it is irrelevant whether or not such data have undergone specific technical processing.

While biometric data and body data are particularly sensitive categories of data per se due to the special way in which they are generated, many other data may be used to record, infer, or apply some kind of differential treatment based on particularly sensitive characteristics of a natural person. Such sensitive characteristics include racial or ethnic origin, migration status, political opinions, religious or philosophical beliefs, disability, state of health, emotional or psychological state, trade union membership, a person's sex life or sexual orientation, or criminal convictions. This list has been inspired both by the list in Article 9(1) of Regulation 2016/679 and by the more recent list in Article 7(1)(e) of Directive 2024/2831. For example, data such as a person's shopping history and browsing behaviour can provide deep insights into their mental health and emotional state. If the processing of personal data of any kind serves such a purpose, it should be considered a high-risk data activity even if the data originally processed do not qualify as special categories of data. Differential treatment based on such sensitive characteristics should include any automated decision making based on personal data that serve, taking account of the algorithms used for processing, as a proxy for the sensitive characteristics.

Other examples of high-risk data processing include systematic monitoring of a publicly accessible space, which was also mentioned previously in Article 35 of Regulation 2016/679, as well as transferring personal

data to third countries based on Article 49(1)(a) to (d). The latter should include only the deliberate transfer of personal data, by active or passive behaviour, such as by actively sending data to a controller or processor in a third country or allowing such a controller or processor in a third country to retrieve personal data. However, it should not include the type of accidental transfer that many controllers using products or services from third country providers cannot avoid by any reasonable means.

Better protection by enabling effective consent management

After Article 8 of Regulation 2016/679, the following Article 8a is inserted:

Article 8a

Large-scale controllers engaging in high-risk data processing

1. Where a large-scale controller engages in high-risk data processing or makes personal data available, directly or indirectly, to other controllers that will engage in high-risk data processing based on the data subject's consent within the meaning of Article 6(1)(a) or Article 9(2)(a), this Regulation and Directive 2002/58/EC shall apply with the following modifications:

a. the data subject's consent to the collection or use of personal data shall expire, at the latest, after [one] year from its provision, renewable for an unlimited number of times, unless consent was given for a purpose that is time-limited by its very nature and the time-limit does not exceed [five] years;

b. the data subject shall receive a copy of consent, including the name and contact details of the controller, the purposes of data processing, information on the right to withdraw consent and the data subject's rights under this Regulation in a clear and transparent manner, by means that minimise the processing of personal data and in a commonly used and machine-readable format that allows for long-term automated consent management by the data subject, including withdrawal of consent and exercise of the data subject's rights, where technically possible;

c. the controller shall be under an obligation to cooperate with a data intermediation services provider within the meaning of Article 10 of Regulation 2022/868 that has been indicated by the data subject, or an equivalent system of automated consent management used by the data subject, so that any consent given by the data subject and any withdrawal of consent or exercise of the data subject's rights can effectively be managed by that data intermediation services provider on behalf of the data subject or through the equivalent automated consent management system;

d. the controller shall be under an obligation to ensure that recipients to whom the personal data have been disclosed are notified of any withdrawal of consent, rectification or erasure of personal data or restriction of processing by automated means, unless this proves impossible or involves disproportionate effort;

e. the controller shall maintain at least one online interface accessible to the public and shall equip all existing online interfaces accessible to the public with technical means that are easy to find, understand and apply by the relevant data subjects and that allow at least for the following:

i. the withdrawal of consent and the exercise of the data subject's rights; and

ii. the indication of a data intermediation services provider or automated consent management system of the data subject's choice within the meaning of point (c).

The Commission shall adopt delegated acts to specify the details of these obligations, or issue, in accordance with Article 10 of Regulation 1025/2012, a standardisation request covering the details of these obligations.

2. **The large-scale controller shall indicate on all existing online interfaces accessible to the public in a clear and transparent manner and in machine-readable format that it qualifies as a large-scale controller and is thus subject to the specific obligations under this Article. This information shall, in any case, be included in the information to be provided to the data subject under Articles 13 or 14.**

3. **A large-scale controller that engages in high-risk data processing shall, vis-à-vis the data subjects concerned, comply with the obligations under paragraph (1) also with regard to processing not qualifying as high-risk data processing that is based on the data subject's consent.**

4. **Where two or more controllers, including the controller initially collecting the personal data, are subject to the obligations under paragraph 1 with regard to the same personal data, they can agree that the collecting controller fulfils certain obligations under points (b) to (d) of paragraph (1) also on behalf of other controllers. Such an arrangement must be clearly documented and must ensure full and effective compliance with the obligations under paragraph (1) by all controllers involved. Article 26 remains unaffected.**

Proposed accompanying recitals:

While high-risk data processing operations, such as trading personal data, generally pose an increased risk to the fundamental rights of data subjects, the overall risk is significantly aggravated when they are carried out by large-scale data controllers. This is not only because more data subjects are affected, but also because such controllers have more possibilities to combine different data sets and to make sophisticated use of the data. At the same time, given their size and degree of specialisation and sophistication, large-scale controllers can be expected to comply with enhanced obligations. Therefore, Article 8a sets out a number of additional safeguards to complement the existing obligations under Regulation 2016/679 in cases where the processing of personal data is based on the consent of data subjects. Where a large-scale controller engages in some high-risk data activities, but also in other data activities that do not pose a high risk, that large-scale controller shall comply with the enhanced obligations also with regard to personal data not affected by the high-risk data activities as far as such processing is equally based on the data subject's consent. This is to avoid data subjects being confused by the scope of, for example, withdrawal of consent.

Under Articles 6 to 8 of Regulation 2016/679, the data subject's consent, once given, is normally not subject to expiration, except where the purpose for which it has been given expires. Furthermore, neither the information to be provided to the data subject nor the consent itself have to be recorded on a durable medium, which is why data subjects, eg when they have given consent by clicking 'OK' on an online interface, normally cannot trace back to whom they have given consent, and for what. Even where they remember to whom they have given consent, it is often difficult to find and use the right mechanism for withdrawing consent or making use of data subjects' rights, and controllers may have passed data on to other controllers or processors. While, theoretically, data subjects could rely on the support of a data intermediation services provider within the meaning of Article 10 of Regulation 2022/868, there is no obligation under Regulation 2016/679 for the controller to cooperate with such a service provider.

It is for all these reasons that Article 8a provides that, where a large-scale controller engages in high-risk data processing based on the data subject's consent, consent shall normally expire, at the latest, after [one] year from its provision, but renewable for an unlimited number of times. The only exception is where consent had been given for data processing that is time-limited by its very nature, such as profiling related to a particular educational programme with a fixed duration, in which case new consent needs to be sought only after [five] years. Needless to say, this is without prejudice to earlier expiry where the purpose for which consent had been given is no longer relevant.

Data subjects shall normally receive a copy of consent and basic information in a way that allows

long-term storage and consent management, which will normally mean that the information must be provided on a durable medium. However, this must be done in a way that does not create further data protection risks. A standard way of achieving this on the Internet could be the use of technical facilities within the browser used by the data subject. Under no circumstances should a large-scale controller use this obligation as a pretext to request the data subject's e-mail address or telephone number in situations where that address or number is not already lawfully requested for other reasons. The information must be given in a clear and transparent manner so that it can be easily understood by a human reader, but also in a commonly used and machine-readable format that allows for long-term automated consent management by the data subject.

The controller shall be under an obligation to cooperate with a data intermediation services provider that has been indicated by the data subject so that any consent given by the data subject and any exercise of the data subject's rights can effectively be managed by that data intermediation services provider on behalf of the data subject, which includes the provision of appropriate technical means. The same applies where the personal information is not managed by a separate legal entity, but where the data subject uses a software solution, including any AI, to achieve the same objective. In addition, the controller shall maintain an online interface accessible to the public and shall equip this interface with simple technical means that allow data subjects to withdraw consent and exercise other rights, including indicate a data intermediation services provider or software solution.

It is important that data subjects and authorities know about the fact that the large-scale controller is subject to enhanced obligations under Article 8a. While it is for each controller to ensure whether or not they qualify as large-scale controller, once this question has been answered in the affirmative, the large-scale controller shall indicate on all existing online interfaces accessible to the public in a clear and transparent manner and in machine-readable format that it qualifies as a large-scale controller and is thus subject to the specific obligations under this Article. The information shall, in any case, be included in the information that has to be provided to the data subject under Articles 13 or 14 of Regulation 2016/679

Often, there is a situation of multiple controllers in a data value chain, where more than one controller is subject to the enhanced obligations. In this case, it might be technically challenging and confusing as well as burdensome for the data subjects if every controller had to comply separately with all the enhanced obligations, for example if every controller had to provide a copy of consent on a durable medium. This is why controllers should be allowed to agree that the collecting controller fulfils certain obligations also on behalf of other controllers. Such an arrangement must be clearly documented and must ensure full and effective compliance with the enhanced obligations by all controllers involved.

Visibility and traceability of data traders

After Section 4 of Chapter IV of Regulation 2016/679, the following Section 5 is inserted:

Section 5

Special obligations of very large large-scale controllers and processors

Article 39a

Database of data traders

1. Large-scale controllers engaging in trading personal data, as well as large-scale processors acting on behalf of controllers trading personal data, with regard to at least [1,000,000] data subjects in the Union shall register in an electronic database set up and maintained by the Commission, in collaboration with the Member States and in consultation with the Board referred to in Article 68.

2. The database shall be accessible and publicly available in a user-friendly manner, and the information should be easily navigable and machine-readable. The database shall be equipped with a functionality that allows for the withdrawal of consent or exercise of the data subject's rights by automated means.

3. The Commission shall adopt delegated acts to specify the details of the information to be entered into the database by the large-scale

controller or processor or, where applicable, by the authorised representative, as well as the functionalities within the meaning of paragraph 2 and the measures that must be taken by large-scale controllers and large-scale processors within the meaning of paragraph 1 to enable those functionalities.

4. The Commission shall be the controller of the EU database. It shall make available to large-scale controllers and processors adequate technical and administrative support.

Proposed accompanying recital:

In the data economy, data subjects are often faced with the problem that players remain invisible to them. To a certain extent, this problem is already addressed by the enhanced obligations established under Article 8a. These obligations shall be complemented, however, by the obligation of very large large-scale controllers that engage in data trading with regard to at least [1,000,000] data subjects in the Union to register in an electronic database set up and maintained by the Commission, in collaboration with the Member States. The same shall apply to very large-scale processors that assist controllers (regardless of their size) specifically with the trading of personal data. This requires the large-scale processor to be aware of the data trading and to provide specific assistance with it. Conversely, a large-scale processor that only provides web hosting or cloud storage services for a data trader should not be subject to the registration obligation.

The database will be accessible and publicly available in a user-friendly manner. This is to ensure that data traders whose activities affect a significant number of data subjects in the Union are easily identifiable and that, for example, access requests or requests for erasure under Regulation 2016/679 can easily be addressed directly to the registered controllers. Registered controllers could be addressed in a variety of different ways, including by automated means and with the support of data intermediation services providers. In order to make this technically possible, the database shall be equipped with a functionality that allows for the withdrawal of consent or exercise of the data subject's rights by automated means. The Commission shall adopt delegated acts to specify the details of the information to be entered into the database by the large-scale controller or processor, or by the authorised representative where applicable, as well as the functionalities of the database and the measures required by the large-scale controller or processor to enable these functionalities.

Mandatory audits for the very large players

Article 39b

Mandatory data protection audits

1. Large-scale controllers engaging in high-risk data processing, as well as large-scale processors acting on behalf of controllers engaging in high-risk data processing, with regard to at least [10,000,000] data subjects in the Union shall be subject, at their own expense and at least once a year, to independent audits to assess compliance with the obligations set out in this Regulation. This audit can be combined with an audit required under Article 37 of Regulation 2022/2065.

2. Large-scale controllers and large-scale processors covered by paragraph 1 shall afford the organisations carrying out the audits pursuant to this Article the cooperation and assistance necessary to enable them to conduct those audits in an effective, efficient and timely manner, including by giving them access to all relevant data and premises and by answering oral or written questions. They shall refrain from hampering, unduly influencing or undermining the performance of the audit.

Such audits shall ensure an adequate level of confidentiality and professional secrecy in respect of the information obtained from the large-scale controllers and large-scale processors and third parties in the context of the audits, including after the termination of the audits. However, complying with that requirement shall not adversely affect the performance of the audits and other provisions of this Regulation, in particular those on transparency, supervision and enforcement. Where necessary the audit report and the audit implementation report shall be accompanied with versions that do not contain any information that could reasonably be considered to be confidential.

3. Audits performed pursuant to paragraph 1 shall be performed by organisations which:

a. are independent from, and do not have any conflicts of interest with, the large-scale controller or large-scale processor covered by paragraph 1 concerned and any legal person connected to that controller or processor; in particular:

i. have not provided non-audit services related to the matters audited to the large-scale controller or large-scale processor covered by paragraph 1 and to any legal person connected to that provider in the [12] months' period before the beginning of the audit and have committed to not providing them with such services in the [12] months' period after the completion of the audit;

ii. have not provided auditing services pursuant to this Article to the large-scale controller or large-scale processor covered by paragraph 1 and any legal person connected to that controller or processor during a period longer than [five] consecutive years; and

iii. are not performing the audit in return for fees which are contingent on the result of the audit;

b. have proven expertise in the area of data protection and have the necessary technical competence and capabilities; and

c. have proven objectivity and professional ethics, based in particular on adherence to codes of practice or appropriate standards.

4. Large-scale controllers and large-scale processors covered by paragraph 1 shall ensure that the organisations that perform the audits establish an audit report for each audit. That report shall be substantiated, in writing, and shall include at least the points listed in Annex III.

5. Where the organisation performing the audit was unable to audit certain specific elements or to express an audit opinion based on its investigations, the audit report shall include an explanation of the circumstances and the reasons why those elements could not be audited.

6. A large-scale controller or large-scale processor receiving an audit report that is not 'positive' shall take due account of the operational recommendations or remediation actions addressed to them with a view to taking the necessary measures to implement them. They shall, within one month from receiving those recommendations or remediation actions, adopt an audit implementation report setting out those measures. Where they do not implement the operational recommendations or remediation actions, they shall justify in the audit implementation report the reasons for not doing so and set out any alternative measures that they have taken to address any instances of non-compliance identified.

7. The Commission is empowered to adopt delegated acts to supplement this Regulation by laying down the necessary rules for the performance of the audits pursuant to this Article, in particular as regards the necessary rules on the procedural steps, auditing methodologies and reporting templates for the audits performed pursuant to this Article.

Proposed accompanying recital:

For even larger large-scale controllers or large-scale processors that engage in high-risk data processing (such as profiling) with regard to at least [10,000,000] data subjects in the Union, there should be mandatory independent audits. The provision on audits has been aligned with the parallel provision in Article 37 of Regulation 2022/2065 for providers of very large online platforms and of very large online search engines. Details are included in a new Annex III.

[Note: Annex III is not included in this document]

IV. Modular proposals for facilitating innovation

1. Removing uncertainties in the context of special categories of personal data

Restricting Article 9 to sensitive processing operations

Article 9 paragraph 1 of Regulation 2016/679 shall be replaced by the following:

1. Insofar as the processing of personal data

a. concerns data that is biometric or genetic in nature and allows the unique identification of a natural person; or

b. concerns data that is inherently and specifically linked with sensitive characteristics; or

c. is for a purpose that is related to sensitive characteristics, in particular to record or infer sensitive characteristics or apply any differential treatment based on sensitive characteristics,

such processing shall be lawful only if, and to the extent that, at least one of the cases in paragraph 2 applies.

Paragraph 4 of Article 9 shall be deleted, and in paragraph 3 the words 'Personal data referred to in paragraph 1 may be processed for' shall be replaced by 'Processing of personal data referred to in paragraph 1 may occur for'.

Proposed accompanying recitals:

Article 9 of Regulation 2016/679 so far prohibits the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning the sex life or sexual orientation of a natural person. Article 9(2) lists a number of narrowly defined exceptions to this rule, which may be further restricted by Member States. The Court of Justice (C-184/20, C-21/2) has ruled that Article 9 of Regulation 2016/679 must be interpreted as including personal data that may indirectly reveal sensitive information about a natural person. This could potentially affect a wide range of everyday activities, such as the operation of an online bookshop or a grocery store where, for example, the books ordered could reveal a person's political views, or where a person orders lactose- or gluten-free food, which could reveal a person's health status. In addition, the Court has ruled that mixed datasets containing some special category data must comply with the stricter requirements of Article 9 as a whole (C-252/21).

In order to preserve the protective function of Article 9 of Regulation 2016/679 and to avoid an inflationary collection of 'explicit consent' for the most mundane activities, the provision should apply to the processing of sensitive personal data only where the biometric or genetic data allows the unique identification of a natural person or is inherently and specifically linked to sensitive characteristics. This is the case, for example, with health records, but not with a holiday photo of a person which, among other things, reveals the person's state of health (eg because the person wears glasses or walks on crutches). Article 9 of Regulation 2016/679 should also apply where the data are used for a purpose related to sensitive characteristics, in particular to infer sensitive characteristics or apply any differential treatment based on sensitive characteristics. By contrast, where data that could potentially reveal sensitive characteristics are used for purposes unrelated to sensitive characteristics, such as the performance of a sales contract or the indiscriminate analysis of large amounts of data to train a general-purpose AI model, Article 9 of Regulation 2016/679 does not apply. Needless to say,

where a data processing operation is exempt from the scope of application of Regulation 2016/679 by virtue of Article 2a or 2b, also Article 9 of Regulation 2016/679 does not apply.

Additional grounds for the permitted processing of special categories of personal data

In Article 9 paragraph 2 the words 'Paragraph 1 shall not apply if' shall be replaced by 'Processing of personal data within the meaning of paragraph 1 is lawful if', and after point j, the following points k and l shall be inserted:

k. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

l. processing is necessary for detecting and correcting biases or avoiding discrimination and appropriate safeguards are in place to prevent any use of the data for other purposes up to the point when the data are irreversibly anonymised or erased.

Proposed accompanying recitals:

Article 9(2) of Regulation 2016/679 previously failed to allow the processing of special categories of personal data in cases where such processing was necessary for the performance of a contract to which the data subject was a party, or for taking steps at the request of the data subject prior to entering into a contract. This meant that explicit consent had to be given for many day-to-day activities, even when the data subject had deliberately and knowingly entered into a contract involving the processing of special categories of data (eg health data), creating an unnecessary administrative burden and causing uncertainty. This is why this legal basis, with the strict interpretation given to it in the context of Article 6(1)(b), has been added to Article 9(2).

AI and related technologies have the potential to discriminate, including on the basis of sensitive characteristics, many of which are also protected characteristics under Union or Member State anti-discrimination law. It is therefore essential that such technologies are designed to avoid discrimination and that appropriate measures are taken at the design stage. This may require the processing of sensitive data, where the use of synthetic or anonymous data is not sufficient. While Article 10(5) of Regulation 2024/1689 has made this possible under certain conditions, the scope of the provision is limited to high-risk AI systems as defined in Regulation 2024/1689. However, the need to avoid bias and discrimination is not limited to high-risk AI systems. Therefore, Article 9 of Regulation 2016/679 should also not apply to the processing of sensitive personal data where the processing is carried out for the sole purpose of detecting and correcting bias or avoiding discrimination, provided that the processing of sensitive personal data is necessary for this purpose and that appropriate safeguards are in place to prevent any use of the data for other purposes, until such time as the data are irreversibly anonymised or erased. As this new provision is broader in scope than Article 10(5) of Regulation 2024/1689, the latter can be deleted.

2. Removing uncertainties in the context of new technologies

Legal basis for training AI and similar activities

After paragraph 4 of Article 6, the following paragraph 5 is inserted:

5. A controller engaging in the processing of large amounts of data in an indiscriminate manner and for purposes not related to data subjects as identified or identifiable natural persons, including the training of AI models or systems, may rely on a legal ground which is given with regard to the vast majority of the data if both of the following requirements are met:

a. verifying the actual existence of a legal ground for all personal data involved would cause effort that is disproportionate in the light of, in particular, the extent to which the logic used by the AI model or system is related to data subjects as identified or identifiable natural persons, the likely

risk posed for data subjects, and the purposes for which the AI is created; and

b. appropriate safeguards have been applied that ensure compliance with the principles set forth in Article 5 to a degree that is reasonable in the circumstances.

The Commission is empowered to adopt delegated acts to further specify the appropriate safeguards referred to in point b or issue, in accordance with Article 10 of Regulation 1025/2012, a standardisation request covering the requirements to be met by appropriate safeguards.

Proposed accompanying recitals:

A controller processing personal data for purposes, including the training of AI models or systems, that involve the processing of large amounts of data in an indiscriminate manner and for purposes not related to data subjects as identified or identifiable natural persons may face significant difficulties in ensuring full compliance with Regulation 2016/679 for each individual data point. In order not to create a situation where such data activities can no longer be carried out in the Union, even if controllers have applied all reasonable and proportionate safeguards, this Regulation provides that a controller may rely on a legal basis in Article 6 or Article 9 of Regulation 2016/679, including on Article 6(4), which applies to the bulk of the data if two requirements are met: First, the situation must be such that verifying the actual existence of a legal basis for all the personal data concerned would entail a disproportionate effort, in particular taking into account the extent to which the logic used by the AI model or system relates to data subjects as identified or identifiable natural persons, the likely risk to data subjects and the purposes for which the AI is created. Second, the controller must have implemented appropriate safeguards to ensure compliance with the principles set out in Article 5 of Regulation 2016/679 to the extent reasonable in the circumstances. For example, where the controller engages in the scraping of data that is freely available on the internet, the controller can normally be expected to use available technology to anonymise data that is manifestly personal data, with the exception of personal data published in a way giving rise to the reasonable expectation that they have been manifestly made public by the data subject (such as entries on 'Wikipedia' and the like). The Commission is empowered to adopt delegated acts to further specify the appropriate safeguards referred to.

More targeted data subjects' rights in the context of AI

After Article 23 of Regulation 2016/679, the following Article 23a is inserted:

Article 23a

Data subjects' rights in the context of general-purpose AI and similar technologies

1. Exercise of data subjects' rights under Articles 15 to 18, 20 and 21 with regard to processing of personal data that occurs exclusively within an AI model or system or similar technology in a way that makes them an integral part of the technology, up to and including the point when output is generated, shall not cause efforts that are clearly disproportionate. When determining the appropriate scope of these rights, factors to be taken into account include the extent to which the logic used by the technology is related to data subjects as identified or identifiable natural persons, the actual risk posed for data subjects, the amount of investment made, the compliance with data protection and other law in developing the technology, and the purposes for which the technology has been created.

2. Where personal data are processed within an AI model or system or similar technology in a way that makes them an integral part of the technology, data subjects shall in any case have the right to request from providers of the technology prompt and effective remedial action where they can demonstrate that the technology:

a. is reasonably likely to be used with regard to the data subject; and

b. generates, in a systematic manner, output relating to the data subject as an identified or identifiable natural person that:

i. **is likely to harm the data subject's reputation, intrude upon the data subject's private and family life or otherwise manifestly harm the data subject's rights and legitimate interests in a way that would be unlawful if done by a human ('right against harmful mention'); or**

ii. **imitates, without the data subject's explicit consent, characteristic personal features such as voice, facial expressions or literary or artistic style that would render the data subject identified or identifiable, whether or not such features are protected by the law of intellectual property ('right not to be cloned').**

3. **Nothing in this Article shall affect data subjects' rights with regard to personal data used as training, validation, testing or input data as far as they exist outside the AI model or system or similar technology, as well as to the use, including mere storage, of output generated by the technology, subject to any exemptions under this Regulation or under other Union or national law.**

Proposed accompanying recitals:

Complying with the rights of data subjects under Regulation 2016/679 in the context of general-purpose AI and similar technologies, which may include distributed ledger technologies, may pose a serious challenge where the personal data exists within the model or system in such a way that it becomes an integral part of the model or system. For example, due to the opacity of AI models or systems, it may not be possible to provide access to or transfer the data in accordance with Articles 15 or 20 of Regulation 2016/679, or to erase the data in accordance with Article 17 where the processing was based on consent and that consent is withdrawn. In such situations, complying with the full set of data subjects' rights under Regulation 2016/679 may involve disproportionate efforts or even be impossible without destroying the AI model or system, in which case a data subject should be able to exercise such rights only within the limits of what is still possible and proportionate. What is considered 'disproportionate' will depend on the circumstances of the individual case. Factors to be taken into account include the extent to which the logic used by the AI model or system relates to data subjects as identified or identifiable natural persons, the actual risk posed to data subjects, the level of investment made, compliance with data protection and other laws, and the purposes for which the AI model or system was created. For example, if there has been manifest disregard for data protection law in the creation of the AI model or system, the relevant providers should not be allowed to rely on the exemption. With regard to the information obligation, it is understood that the same effect is already created by Article 14(5)(b) of Regulation 2016/679.

In order to respond to the specific situation that data subjects may find themselves in in the face of general-purpose AI that has been trained with personal data, two new rights are introduced that are available to data subjects whenever personal data are processed within an AI model or system in a way that makes them an integral part of the model or system. They have, again, been inspired by the ALI-ELI Principles. These rights apply regardless of whether data subjects continue to enjoy their rights under Regulation 2016/679. Where an AI system is built on the basis of a general-purpose AI model, the obligations under Article 23a lie with the AI system provider. In order to take remedial action, the AI system provider will often have to rely on the information and documentation provided by the general-purpose AI model provider in accordance with Article 53 of Regulation 2024/1689.

The new 'right against harmful mention' becomes relevant where an AI model or system is reasonably likely to be used in relation to data subjects, and where the model or system generates output in relation to data subjects in a systematic way that is likely to cause manifest harm and would be unlawful if done by a human. This can happen in two ways. The first possibility is that the system ingested personal data during training and 'memorised' it. The second possibility is that the system produces information that is statistically plausible but false about the person, and this can be systematic depending on the statistical distributions in the training data (eg biases that link certain types of names with certain stereotypical behaviours). If this happens, data subjects have the right to require providers to take

prompt and effective remedial action. For example, if a chatbot, when asked about a particular person, falsely suggests that that person is involved in criminal activity (eg because the person is a journalist who regularly reports on serious crime), this could give rise to such a right. Due to the existence of the second possibility just mentioned, simply removing data subjects' personal data from the training data may not be enough to eliminate harmful effects. The most technically feasible method of dealing with this issue currently is to address the problem at generation time (ie identify and modify the harmful output or continue generating until something non-harmful is produced). The boundaries of what is still lawful should not be defined by data protection law, but by other laws, and should be defined in a way that is comparable to the situation when, for example, something is published by a human.

The 'right not to be cloned' means that where an AI model or system is reasonably likely to be used with respect to a data subject, and where that model or system imitates, without the explicit consent of the data subject, characteristic personal features, such as voice, facial expression or literary or artistic style that would make the data subject identifiable or recognisable, regardless of whether or not such features are protected by intellectual property law, data subjects have the right to require providers to take prompt and effective remedial action. It should be noted that this only applies if the data enabling imitation are contained in the model or system. Therefore, the right not to be cloned cannot be invoked against software which, for example, only processes audio or video material fed into the system (eg in order to produce a 'deep fake'). Similarly, the right not to be cloned cannot be invoked as a collective right, eg by the creative professions, but only where a particular individual is identifiable.

Data subjects will continue to have all the rights and remedies afforded to them under Regulation 2016/679 with regard to personal data used as training, validation, testing or input data, to the extent that they exist outside the AI model or system. The same applies to the use of any output generated by the AI model or system. This is particularly important, as Article 22 of Regulation 2016/679 must continue to apply to automated decision making. Similarly, where output relating to an identified or identifiable natural person is stored or otherwise processed by the operator of the AI, the rights of data subjects to request, for example, access or erasure must continue to apply.

3. Reducing differences in implementation and enforcement

A new conflict-of-laws provision

After Article 3 of Regulation 2016/679, the following Article 3a is inserted:

Article 3a

Applicable law

1. In a conflict of laws between different Member States, a controller's or processor's obligations under data protection law shall be governed by the law of the Member State where, at the relevant point in time, the controller has their place of establishment or habitual residence. Where two or more joint controllers have their place of establishment or habitual residence in different Member States, they shall, in the arrangement referred to in Article 26(1), determine in a transparent manner the law of the Member State in which any of the controllers has its place of establishment or habitual residence as the applicable law, unless that controller plays an insignificant role compared with the other controllers.

2. In situations not covered by paragraph (1), a controller's or processor's obligations under data protection law shall be governed by the law of the Member State where the data subject has their habitual residence.

3. As far as data protection law refers to laws addressing matters other than data protection, such as the law of contract or law conferring on the controller a specific official authority, the law governing that other matter shall apply. *[Option: In the context of employment, a controller's or processor's obligations under data protection law shall be governed by the law referred to by Article 8 of*

Regulation 593/2008 or that would be referred to by Article 8 of Regulation 593/2008 if an employment contract were concluded.]

4. **Where it is clear from all the circumstances of the case that the processing of personal data is manifestly more closely connected with a country other than that indicated in paragraphs (1) to (3), the law of that other country shall apply.**

Proposed accompanying recitals:

While Regulation 2016/679 generally provides for a harmonised data protection regime across the Union, there are situations where there is room for diverging rules at national level because Member States may deviate from the default regime in defined ways. Examples include the age at which children can consent to the processing of their personal data, stricter rules for special categories of personal data or special data protection rules for the area of scientific or historical research. For controllers operating in different Member States, the need to comply with a number of different legal regimes at the same time can significantly increase the administrative burden. This has proved to be particularly detrimental in the field of scientific research, clearly hampering research and innovation in Europe to the detriment of European interests. Therefore, in line with Recital 153, a controller should be able to rely on the data protection law of the Member State where it is established or has its habitual residence. Where two or more joint controllers have their place of establishment or habitual residence in different Member States, they shall determine the applicable law in a transparent manner, provided that it is the law of a Member State in which one of the controllers playing a more than an insignificant role has its place of establishment or habitual residence. Where the controller has their place of establishment or habitual residence in a third country, however, the law of the habitual residence of the data subject shall apply instead as otherwise the standard of protection afforded to data subjects in the Union could be undermined.

There are also many situations where Member State law can perform an implementing function, for example by providing a legal basis under Article 6(1) (c) or (e). In this case, a controller may rely on such Member State law only if that law is applicable in accordance with the relevant conflict-of-law rules, which may result from legislation such as Regulations 864/2007 or 593/2008 or from Union or Member State law with a defined territorial scope. *[Option: As Member States have certain freedoms to impose stricter provisions than under Regulation 2016/679 in the context of employment, a controller's or processor's obligations under data protection law shall be governed by the law governing the individual employment contract, which is determined by Article 8 of Regulation 593/2008. Where an employment contract has not yet been concluded, the applicable law should be the law that would apply to the employment contract if it were concluded.]*

Since the choice of the general connecting factor could create incentives to artificially relocate to a country whose data protection law is particularly favourable to controllers, another law should apply where it is clear from all the circumstances of the case that the processing of personal data is manifestly more closely connected with a country other than that in which the controller is established. This should be interpreted narrowly so as not to undermine the general rule and should be reserved mainly for cases of obvious abuse.

Centralising certain tasks of supervisory authorities

Paragraphs 4 to 6 of Article 35 of Regulation 2016/679 shall be deleted and paragraph 3 shall be replaced by the following:

3. **A data protection impact assessment referred to in paragraph 1 shall be required, in particular, in the case of high-risk processing that occurs systematically and on a large scale. The Board referred to in Article 68 shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The Board may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required.**

After Article 51, the following Article 51a is inserted:

Article 51a

EU Data Protection Authority

The Commission shall set up the EU Data Protection Authority as an independent supervisory authority at Union level that shall have powers to supervise and enforce this Regulation against large-scale controllers and processors that are subject to the registration requirement under Article 39a or the audit requirement under Article 39b and active in at least two Member States. Where the EU Data Protection Authority has not initiated proceedings for the same infringement, the competent authority of a Member State shall have powers to supervise and enforce the obligations under this Regulation with respect to those large-scale controllers or processors. Supervisory authorities in the Member States and the EU Data Protection Authority shall supervise and enforce the provisions of this Regulation in close cooperation.

Proposed accompanying recitals:

As Article 35 of Regulation 2016/679 has stood until now, national or – in some Member States – even regional data protection authorities have been entrusted with issuing their own 'black-lists' of data processing operations that trigger an obligation to carry out a data protection impact assessment, as well as of 'white-lists' of processing operations that definitely do not trigger such an obligation. This has resulted in additional fragmentation of the implementation of Regulation 2016/679, with no good reason. This is why the black-lists should largely be provided by the European legislator itself, listing instances of high-risk processing in Annex I. Otherwise, the competence for publishing black-lists and white-lists should lie with the European Data Protection Board.

In order to accelerate proceedings, ensure effective enforcement and reduce disparities in enforcement between Member States, a centralised, independent EU Data Protection Authority set up by the Commission shall have powers to supervise and enforce Regulation 2026/679 against large-scale controllers and processors that are subject to the registration requirement under Article 39a or the audit requirement under Article 39b and active in at least two Member States. Where the EU Data Protection Authority has not initiated proceedings for the same infringement, the competent authority of a Member State shall continue to have powers to supervise and enforce the obligations under this Regulation with respect to those large-scale controllers or processors. Supervisory authorities in the Member States and the EU Data Protection Authority shall supervise and enforce the provisions of this Regulation in close cooperation.

An illustrative list of legitimate interests

The second subparagraph of Article 6(1) of Regulation 2016/679 shall be replaced by the following:

An illustrative list of legitimate interests within the meaning of point (f) of the first subparagraph is included in Annex II; the Commission is empowered to adopt delegated acts to amend Annex II by adding, deleting or modifying use-cases of legitimate interests, after having consulted the Board referred to in Article 68. Point (f) of the first subparagraph shall not apply to processing carried out by public authorities where they act in performance of sovereign powers.

The following Annex II is added to Regulation 2016/679:

ANNEX II

Legitimate interests within the meaning of point (f) of the first subparagraph of Article 6 paragraph 1 include, but are not restricted to:

1. Legal and Regulatory Compliance

a. preventing, detecting or investigating fraud and other criminal activities;

b. ensuring workplace safety and security (eg, CCTV monitoring in public areas of the workplace or monitoring premises with sensitive operations);

c. conducting audits or compliance checks;

d. reporting illegal activities or threats to public safety to authorities;

e. cooperating with authorities in situations of emergency.

2. Business Operations and Management

a. ensuring the proper functioning of equipment, IT systems or infrastructure;

b. ensuring network and information security (eg, preventing unauthorised access or cyberattacks) and preventing misuse of services or systems (eg, detecting bots or spam);

c. protecting the controller's or a third party's assets, reputation, or intellectual property;

d. establishing, exercising, or defending legal claims;

e. monitoring business performance or productivity.

3. Research and Development

a. conducting scientific or historical research;

b. improving products or services (eg, based on customer feedback);

c. developing new technologies or services (eg, training, validating or testing of artificial intelligence);

d. clinical trials;

e. archiving or statistical activities in the public interest.

4. Distribution and Marketing

a. ensuring seamless transactions and user experiences on websites or apps;

b. maintaining customer records for service continuity;

c. conducting market research or customer satisfaction surveys;

d. measuring the effectiveness of marketing campaigns.

5. Business Transactions

a. transfers of employee, customer or supplier files within a group of companies;

b. carrying out mergers, acquisitions, or similar business transactions;

c. conducting due diligence in business transactions;

d. assignment of claims, or provision of claims as a security, within common financial transactions.

The fact that a processing operation is covered by subparagraph 1 does not exempt the controller from ensuring that the processing operation is necessary for the purposes of the relevant legitimate interests pursued by the controller or by a third party, and that the interests are not overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. In doing so, the controller shall take into account, among others, the possible consequences of the intended processing for data subjects and the existence of appropriate safeguards.

Proposed accompanying recitals:

In order to enhance legal certainty and ensure a harmonised interpretation of the concept of legitimate interests under Regulation 2016/679, an illustrative list of processing activities is provided that may, in principle, qualify as legitimate interests within the meaning of point (f) of the first subparagraph of Article 6(1). Such a list, included in Annex II, aims to assist data controllers and supervisory authorities in assessing the applicability of legitimate interests while maintaining the flexibility required to address evolving technological, economic, and societal contexts. The list is not exhaustive, and the inclusion of a processing activity in Annex II does not exempt the controller from conducting the balancing test required under point (f) of the first subparagraph

of Article 6(1). Controllers must still ensure that the processing is necessary for the purposes of the legitimate interests pursued and that such interests are not overridden by the interests or fundamental rights and freedoms of the data subject, particularly in cases involving children.

To ensure that Annex II remains relevant and up to date, the Commission should be empowered to adopt delegated acts to amend the Annex by adding, deleting, or modifying use-cases of legitimate interests, following consultation with the European Data Protection Board. This delegated power will allow the Union to respond effectively to new developments and challenges in data protection while safeguarding the rights of data subjects.

The European Law Institute (ELI) is an independent non-profit organisation established to initiate, conduct and facilitate research, make recommendations and provide practical guidance in the field of European legal development. Building on the wealth of diverse legal traditions, its mission is the quest for better law-making in Europe and the enhancement of European legal integration. By its endeavours, ELI seeks to contribute to the formation of a more vigorous European legal community, integrating the achievements of the various legal cultures, endorsing the value of comparative knowledge, and taking a genuinely pan-European perspective. As such, its work covers all branches of the law: substantive and procedural; private and public.

ELI

EUROPEAN
LAW
INSTITUTE

ISBN: 978-3-9505495-9-1