AK EUROPA

Position Paper
February 2026
Digital

© Getty Images

Digital Omnibus Package

COM(2025) 836
COM(2025) 837

Executive Summary

The proposed Digital Omnibus Package (Omnibus Package VII (COM(2025) 836 and 837 final) is much more than a mere simplification of existing regulations put forward by the Commission. Rather, this package proposes serious changes that threaten to lower the current level of consumer and data protection.

Criticism of the approach taken by omnibus legislation

The Commission is proposing far-reaching changes by means of an accelerated legislative procedure intended for amendments of a purely technical nature. This contradicts the principles of proportionality and subsidiarity that the Commission is required to observe. Without a comprehensive impact assessment and sufficient data and figures to substantiate the need for the proposed provisions, there is a possibility that these two legal acts, COM(2025) 836 and 837 final, could be annulled.

AK has analysed in detail the amendments proposed by the Commission to the General Data Protection Regulation (GDPR) and the Artificial Intelligence Act (AI Act).

The following deteriorations are to be feared:

In the GDPR:

- **Restriction of the scope of application**
  The Commission significantly restricts the classification of pseudonymised data as personal data and, with the power granted to adopt implementing acts, creates further opportunities to define the scope of application more precisely and thus restrict it.

- **Extension of the „research privilege“ through a broad definition of „scientific research“**
  Scientific research is defined too broadly in the Commission's proposal; even predominantly commercial purposes do not prevent classification as scientific research. This unduly extends the privileges already existing for scientific research.

- **Privileging the processing of ‚sensitive data' for AI training and AI operation**
  Special categories of personal data are to be permitted for the purposes of AI development and AI operation. There is no need for such privilege; the current provisions of the GDPR are also sufficient for AI operators.

- **Restriction of the exercise of the right of access**
  According to the Commisson's proposal, the right of access, as the central right of data subjects, is to be restricted in such a way that it may only be requested for data protection purposes.

- **Restriction of the information obligations of controllers**
  Under current law, information obligations can already be restricted if the data subject already has the information. Now, these information obligations are to be restricted even further. This threatens to make it more difficult to exercise data subject rights due to a lack of sufficient information.

- **Facilitation of automated individual decision-making with implications for data subjects**
  Currently, there is a general ban on exclusively automated decisions; automated decisions are only permitted in cases listed by law, such as contractual necessity or the explicit consent of the data subject. The Commission wants to move away from this general ban and make automated decisions easier.

- **Uncertainty due to the division of the previous „cookie“ provision between the GDPR and the e-Privacy Directive**
  The processing of non-personal data in connection with terminal equipment is to remain in the e-Privacy Directive, while the processing of personal data in terminal equipment is to be moved to the GDPR, with new legal grounds for the processing of personal data in terminal equipment also being proposed.

In the AI Act:

- **Extension of exemptions to so-called ‚small mid-cap' companies (SMC)**
  As a product safety law, the AI Act primarily focuses on the risk posed by the AI system and not on the size of the company. The simplifications already in place for small and medium-sized enterprises in the AI Act should therefore not be extended to so-called small mid-cap companies. This could result in important quality assurance measures under the AI act not being applied to high-risk AI systems.

- **AI literacy as a mere recommendation**
  The AI literacy of staff and other persons involved with AI systems must be ensured, otherwise operators will lack the competence to deal with AI systems and the human oversight required under the AI Act will be made considerably more difficult.

- **Extension of the permissibility of processing sensitive data for all AI systems**
  Special categories of personal data (‚sensitive data') should now be processed not only in the area of high-risk AI systems, but generally for providers and operators of all AI systems for the purpose of detecting and correcting biases. This constitutes an impermissible extension and privilege at the expense of the fundamental right to protection of personal data.

- **Elimination of the registration obligation**
  According to the Commission's proposal, AI systems that do not constitute high-risk AI systems from an entrepreneurial perspective should no longer be registered. This removes any protective measures for transparency, public accountability and monitoring.

- **Delay in the date of application**
  The Commission proposes postponing the date of application, which threatens to create further legal uncertainty.

AK's position

With the proposed Digital Omnibus Package VII (COM(2025) 836 final and COM(2025) 837 final), the European Commission intends to make some comprehensive changes to a number of legal acts under the banner of „simplification". The Omnibus Package not only seeks to amend legal acts that have only recently come into force or are not yet fully applicable, such as the Data Act or the Artificial Intelligence Act (AI Act), but also proposes comprehensive changes to important protective provisions in the General Data Protection Regulation (GDPR) without any apparent need.

From AK's point of view, it is important to further develop the innovative strength and competitiveness of the European digital industry in order to strengthen jobs, value creation and digital sovereignty in Europe. However, people must be at the centre of the regulations. Maintaining a high level of data protection and privacy, as well as AI regulation that focuses on clear rules, legal certainty and the protection of users and data subjects, are essential in this regard. Under no circumstances should there be any regression in the existing level of protection.

Criticism of the approach taken by omnibus legislation

With its Digital Omnibus Package, the European Commission is not only presenting targeted and technical changes to various legal acts under the banner of „simplification", but is also proposing comprehensive, far-reaching regulations that in some cases restrict fundamental rights (i.a. Art. 8 on the protection of personal data and Art. 38 on consumer protection in the Charter of Fundamental Rights [CFR]). Under the guise of supposed „simplifications" at a purely technical level, the digital package pursues the weakening and watering down of existing standards oriented towards the common good in a manner that is highly questionable from a democratic point of view.

The Commission's introductory remarks on the two legislative acts COM(2025) 836 and 837 final, stating that the changes are merely technical in nature, that an impact assessment is therefore not necessary and that the present Staff Working Document (SWD(2025) 836 final) is sufficient as a basis, cannot therefore be accepted under any circumstances.

The Commission is using the vehicle of omnibus legislation, which was originally intended for purely technical and minor amendments, for comprehensive changes with far-reaching consequences. It is using an urgent procedure without following the steps required in the ordinary legislative procedure. In accordance with the principles of proportionality and subsidiarity, which must always be observed, i.e. examining whether the proposed legislative act is the only way to achieve the stated objective and is proportionate to the problem analysed and substantiated with facts and figures, a comprehensive public consultation, an impact assessment with additional in-depth examination, as fundamental rights are affected, and an analysis of alternatives are required.

In accordance with Article 2 of Protocol (No 2) on the application of the principles of subsidiarity and proportionality to the Treaty on the Functioning of the European Union, the Commission must conduct extensive consultations before proposing a legislative act. In the case of the Digital Omnibus Package presented here, the proposed amendments to the GDPR and the AI Act were not part of a prior consultation. Only after submitting the legislative proposals did the Commission launch a consultation on this. This approach is by no means in line with the principles of subsidiarity and proportionality. The Better Regulation Toolbox, which the Commission has committed to comply with for the purpose of better law-making, also stipulates that, in order to uphold the principles of subsidiarity and proportionality, a comprehensive impact assessment and extensive consultations and stakeholder consultations must be carried out for a legislative act with such far-reaching proposed amendments (such as restricting the scope of the GDPR). The aim is to gather comprehensive information and evidence to demonstrate and substantiate the need for this proposed legislative act.

With regard to the Omnibus I package, the European Ombudsman has identified several procedural short-

comings, including the European Commission's failure to take into account the Better Regulation Guidelines. In our view, the approach taken to developing the Digital Omnibus package is also characterised by a failure to observe the principles of good governance, which contributes to an unbalanced view of the possible impact of the proposals.

The Commission's approach therefore violates fundamental constitutional principles, which it has reaffirmed in the interinstitutional agreement between Parliament, the Council and the Commission. The inadmissibility of this approach can ultimately be substantiated by ECJ case law. These legal acts therefore carry the risk of annulment, which is why the serious amendments proposed in these legal acts must be rejected on these grounds alone.

- **Article 1 – Data Act:**

The consolidation of the various legal acts on data availability and data management (DA, DGA, ODD, FFDR) is welcomed in principle.

However, the dilution of the independence of data intermediation services is rejected, as their structural independence is intended to contribute to changing the fundamentals of data management by ensuring that data is managed and made available in a neutral manner and without any company's self-interest.

For the same reason, the weakening of the reporting obligations of data altruism organisations is also rejected: only if these organisations are absolutely trustworthy and subject to regulatory oversight can it be ensured that personal data can be made available in areas such as medical research.

General Data Protection Regulation (GDPR)

- **Art. 4 (1) and Art. 41a GDPR – Definition of „personal data" and pseudonymisation**

Under current law, pseudonymised data falls within the scope of the GDPR if the personal reference can be restored. This applies even if only a third party has the necessary assignment rule and can make this assignment (see CJEU case C-582/14 – Breyer). For classification as personal data within the meaning of Art. 4 (1) GDPR, it is therefore not necessary that „all information necessary to identify the person concerned is in the hands of a single person". In addition, according to the CJEU, the term should be understood broadly (see CJEU Case C-413/23 P – EDSB v SRB, paras. 54 and 99). The CJEU explains, among other things, that pseudonymisation – depending on the circumstances of the case – can effectively prevent persons other than the controller from identifying the data subject, so that the data subject is not or no longer identifiable to them. However, data that is not personal in itself can become „personal" data if the controller provides it to other persons who have means that, according to general judgement, are likely to enable the identification of the data subject.

In **Art. 4 (1) of the GDPR**, an addition is now to be made to the definition of „personal data", according to which data is no longer classified as personal if the personal reference cannot be established using reasonably applied methods, for example because only a third party knows the necessary allocation rule.

The abbreviated reproduction of the case law inevitably leads to interpretation problems and potentially to an overly broad and misleading application that disproportionately interferes with the fundamental right to data protection. The classification of pseudonymised data as personal data and thus the scope of application of the GDPR is significantly restricted by this addition. The application of the GDPR can thus be quickly circumvented; controllers can wrongfully remove data from the protection of the GDPR by transferring pseudonymised data to third parties. Furthermore, the proposed wording does not refer to pseudonymisation, but contains very general terms.

Furthermore, it is difficult or even impossible for data subjects to assess whether data relating to a particular company is personal data or not, i.e. whether a company has the means that can reasonably be used. This makes it difficult or virtually impossible for data subjects, but also for any other outsiders, to classify the data within the scope of the GDPR and obscures the resulting possible applicability of data subjects' rights.

This is by no means a contribution to „simplification".

The current definition of personal data in Art. 4 (1) of the GDPR should therefore remain unchanged and not be restricted in any way, in the opinion of AK.

This is also related to the proposed **Art. 41a GDPR**. According to this, the Commission should be granted the power to adopt implementing acts to specify the means and criteria for determining whether data is no longer personal data due to pseudonymisation. AK firmly rejects such a possibility of deciding on the classification within the scope of the GDPR by means of implementing acts. Art. 41a GDPR should therefore be deleted without replacement, as should the proposed addition to Art. 4 (1) GDPR. AK doubts that such a provision would withstand review by the CJEU under Article 263 TFEU, given the principles to be observed, as explained above..

- **Formal comment on Art. 4 GDPR**

The Commission proposes adding several definitions to Article 4, but the numbering is not consecutive. Even taking into account the definitions proposed by the EC in the Omnibus IV package (COM(2025) 501 final), which would insert paragraphs 27 and 28, there are no proposals from the EC for definitions for paragraphs 29 to 31 of Article 4. The consecutive numbering in the present digital omnibus should therefore start with point 29 (instead of point 32) for „terminal equipment".

- **Art. 4 (38) GDPR „scientific research" and information obligations under Art. 13 GDPR**

A new Art. 4 (38) GDPR, which should correctly be numbered as 35, introduces a definition of „scientific research". According to this, any research that supports innovation, such as technological developments, should be understood as scientific. This definition is very broad, with the last sentence even allowing for the possibility of pursuing commercial interests through research. This means that „research" carried out by large corporations, which primarily pursue commercial purposes, also falls under this definition. Such a broad definition of the term „scientific research" has far-reaching consequences, especially since this definition must be read and assessed in conjunction with the newly inserted paragraph 5 in Art. 13 GDPR, but also with the other provisions of the GDPR that relate to scientific research.

Article 13 GDPR regulates the information obligations when collecting personal data from the data subject. According to this provision, data subjects must be informed – in addition to key data on the controller – at the time of data collection about their rights as data subjects, e.g. their right to information and erasure.

According to the newly proposed paragraph 5 of Art. 13, this information shall not be provided in connection with the processing of personal data for scientific research purposes if this is impossible or – with reference to Art. 89 (1) GDPR – involves a disproportionate effort.

Such a broad definition in Art. 4 (38) of the GDPR is therefore to be strictly rejected in view of these far-reaching negative effects, because it means less information for data subjects. In the opinion of AK, there is no need to restrict the information obligations, which is why the proposed Art. 13 (5) GDPR should be deleted without replacement.

Furthermore, the inclusion of the broad definition should not lead to a change in the interpretation of Article 5(1)(b) and (e), Article 9(2)(j), Article 14(5)(b), Article 17(3)(d), Article 21(6) and Article 89 of the GDPR, especially since this term is also used here.

From AK's point of view, as already mentioned at the outset, the current interpretation of the GDPR should not be called into question or even changed to the detriment of the data subjects; the proposed additions to Articles 4 and 13 GDPR should therefore be deleted.

- **Art. 5 GDPR – Principles relating to processing of personal data**

Art. 5 GDPR lays down principles for the processing of personal data. In addition to the principles of data minimisation and accuracy, paragraph 1(b) of the cited provision stipulates the principle of purpose limitation.

In the proposed Art. 5(1)(b) GDPR, the double negative in the last sentence, „*not to be considered incompatible*", is removed and replaced by „*be considered to be compatible*". This change is welcome for reasons of better readability. However, the proposal adds in the last half-sentence that the principle of purpose limitation must be complied with „*independent of the conditions of Article 6(4) of this Regulation*".

Art. 6(4) of the GDPR regulates the possibility of processing personal data for another purpose under certain conditions. According to the proposed addition in Art. 5(1)(b) of the GDPR, this provision is now no longer to be taken into account. AK opposes the proposed addition to Art. 5(1)(b) of the GDPR; there is no objective justification for departing from Art. 6(4) of the GDPR in connection with the principle of purpose limitation; this goes far beyond a mere technical adjustment.

As already noted in relation to the proposed Art. 4(38) GDPR, the broad definition of the term „scientific research" should also be rejected here. This term is also used in Art. 5(1)(b) GDPR, according to which the further processing of personal data for scientific research purposes, among other things, is considered compatible with the original purposes. Such a broad understanding of scientific research purposes undermines the principle of purpose limitation to the detriment of data subjects; this definition must therefore also be rejected in light of Article 5(1)(b) of the GDPR.

- **Art. 9 GDPR – Processing of special categories of personal data**

Art. 9(1) GDPR lays down a prohibition on the processing of special categories of personal data („sensitive data"), e.g. data revealing ethnic origin or philosophical beliefs, biometric data or data concerning health.

Art. 9(2) GDPR regulates the circumstances in which the processing of sensitive data is permitted, e.g. with the explicit consent of the data subject to the data processing.

According to the proposed **Art. 9(2)(k) GDPR**, the processing of these special categories of personal data

should now also be permitted for the development and operation of an AI system or AI model under the premises of the new Art. 9(5) GDPR.

According to this proposed **Art. 9(5) GDPR**, appropriate organisational and technical measures shall be implemented to avoid the collection and otherwise processing of sensitive data. If, however, sensitive data is found in the AI system's data set („residual sensitive data"; see Recital 33 of the proposal), the controller must remove it. If their removal involves disproportionate effort, the controller must at least protect the data from being used to generate output or from being disclosed or otherwise made available to third parties.

The proposed Art. 9(2)(k) GDPR now stipulates the permissibility of processing this remaining sensitive data (which cannot be deleted within the meaning of the proposed Art. 9(5) GDPR) in connection with the development and operation of an AI system or AI model. In addition, the explanations in Recital 33 should be taken into account here, according to which the processing of this residual sensitive data must not be necessary for the processing purpose. If, on the other hand, this sensitive data is necessary, the other exceptions in Article 9(2) must be examined.

In the opinion of AK, this proposed regulation is an unjustified and far too broad attempt to grant privileges in favour of the development and operation of an AI system or AI model. In the AK's view, the proposed additions should therefore be deleted. It is neither reasonable nor justifiable for AI system developers and operators to benefit from such privileges when processing sensitive data. Like any other controller, AI system developers and operators can and should comply with the principles of the GDPR on the protection of fundamental rights to respect for private and family life and the protection of personal data (Articles 7 and 8 of the Charter of Fundamental Rights of the EU).

When processing sensitive data, the exceptions under Art. 9(2)(a) to (j) GDPR should therefore be examined, whereby the exceptions in paragraph 2 must be interpreted narrowly (see CJEU Case C-667/21 – Medizinischer Dienst der Krankenversicherung Nordrhein). The processing of sensitive data subsumed under Article 9(2) GDPR must comply with the general principles regarding the conditions for lawful processing under Art. 6 GDPR within the meaning of Recital 51 to the GDPR and in the light of the case law of the CJEU (see CJEU Case C-667/21 – Medizinischer Dienst der Krankenversicherung Nordrhein).

The processing of sensitive data under Art. 9(2)(k) of the draft GDPR must therefore also fulfil one of the conditions for lawfulness set out in Art. 6(1) GDPR.

This is where the draft Article 88c GDPR comes into play, according to which the controller may rely on a legitimate interest within the meaning of Art. 6(1)(f) GDPR in connection with the development and operation of an AI system or AI model, whereby additional safeguards to be complied with in Article 88c of the draft are also referred to.

In this context, Art. 4a of the draft AI Regulation should also be mentioned, which, according to the EC's proposal, now allows all providers and operators of AI systems to process sensitive data for the purposes of detecting and correcting bias, provided that appropriate safeguards specified therein have been taken.

With regard to the exception under Art. 9(2)(k) of the draft GDPR, it should be noted that new legal terms and unclear wording have been chosen here. The term „*AI model*" is not defined in either the AI Act or the GDPR. In the AI Act, the term is mentioned in connection with general-purpose AI models (GPAI) in Article 51 et seq. of the AI Act. From a technical point of view, an AI model is part of an AI system.

The term „*operation*" in Art. 9(2)(k) and in the drafted paragraph 5 GDPR is also unclear. The AI Act merely defines the term „*operator*" in Art. 3(8) and subsumes all actors addressed in the AI Act under this term. If such an interpretation is also envisaged in the GDPR, this would constitute an excessively broad and, in our opinion, inadmissible exception to the prohibition on the processing of sensitive data.

The addition that sensitive data may be processed for the purposes of developing and operating an AI system or model also raises concerns that AI systems will be used more frequently in future, as sensitive personal data may be processed more easily. The Article 29 Data Protection Working Party has rightly pointed out that the misuse of sensitive data in particular can have more serious consequences for the fundamental rights to privacy and non-discrimination, which can be irreversible and long-lasting for the individual concerned (high potential for harm and abuse). In the context of employment or workers' council activities in particular, a large amount of sensitive data is generated, and employers may have a keen interest in using such information for various reasons (e.g. in return-to-work interviews, investigating the causes of sick leave, health and sick leave data of individual employees, trade union membership or absenteeism). Sensitive data can also be found in everyday consumer life, from smartwatches to orders for medical products, political writings or visits to relevant websites that track users. This data could subsequently be aggregated and used by an AI system to create individual prices, manipulative techniques that exploit „weaknesses", etc. This

data must continue to be subject to a particularly high level of protection, which is why this proposed amendment must be clearly rejected.

AK has no objections to the exception provided for in the newly created **Art. 9(2)(l) GDPR**, according to which the processing of biometric data is permitted if this is necessary for the purposes of confirming the identity of the data subject and the data subject has sole control over the biometric data or the means of verification.

- **Art. 12 GDPR – Transparent information, communication and modalities for the exercise of the rights of the data subject**

Art. 12 GDPR regulates transparent information, communication and modalities for the exercise of the rights of the data subject and refers to the mandatory information under Articles 13 and 14 GDPR and to the communications under Articles 15 to 22 and Article 34 GDPR, i.e. to the rights of data subjects such as the right of access under Article 15 GDPR.

According to the COM proposal, Art. 12(5) GDPR is to be supplemented by the addition „or also, for requests under Article 15 because the data subject abuses the rights conferred by this regulation for purposes other than the protection of their data (...)" According to this, a request for information can be rejected as manifestly unfounded if the data subject abuses the rights conferred by this Regulation for purposes other than the protection of their personal data.

This addition significantly weakens the legal position of those affected. The general right of access is **the central right of data subjects**. Its prominent position is evident in Art. 8(2) sentence 2 of the Charter of Fundamental Rights, which expressly guarantees this right, and in the guarantee of legal protection in Article 47 of the Charter. Any restriction of this right (even if only conceivable) leads to an inadmissible erosion of fundamental rights provisions and must therefore be rejected for this reason alone.

It is to be feared that these planned changes will be particularly disadvantageous for employees as affected parties in an employment relationship with the inherent imbalance of power and, consequently, imbalance of information. In practice, this will result in a massive deterioration of their legal position. Through the use of modern technologies, more and more data about employees is being collected, gathered and technically processed, linked and evaluated. This must not be done without providing the persons concerned with the relevant information. The general right of access is a key right for employees to check the legality of data processing by their employer as the controller, to identify violations of employee data protection or to uncover surveillance. This right also forms the basis for obtaining a copy of their data, such as documents relating to salary calculations, performance data, internal assessments of their person, documents concerning them, or correspondence relating to them. Access to one's own data must be maintained, especially in such a relationship of dependency, and must not be subject to the restriction that this right must be used for „data protection purposes".

In everyday consumer life, too, the right of access is often the only option that can be sanctioned against the controller, also due to legal deadlines, for example, to obtain internal and unjustified third-party access to one's own data, important notes from a telephone conversation or contract documents. If the right of access is not fulfilled, it can be pursued further through the free complaint procedure, thereby „strengthening" the position of the data subject in a power imbalance. In this context, there is already relevant case law on what constitutes permissible information or data copies. The gradual legal certainty gained for data subjects in this way would be lost with the proposed amendment, weakening them not only in terms of data protection law, but also in civil proceedings, equal treatment conflicts, proof of discrimination, etc.

The EU legislator itself has stipulated in Art. 1(2) of the GDPR that the GDPR protects all fundamental rights. The GDPR must continue to enable data subjects to defend their rights and interests on the basis of information about themselves and to compel those in power to be accountable to those subject to their authority.

The exercise of the right of access must therefore continue to be guaranteed in accordance with the case law of the CJEU. In its decision of 26 October 2023, C-307/22, the CJEU clarified that the obligation to provide information also applies if the request for information is justified by purposes other than those specified in the GDPR. A request for information is therefore not „manifestly unfounded" or an abuse of rights if it pursues objectives unrelated to data protection (such as obtaining evidence for subsequent legal proceedings).

According to the case law of the CJEU, a purpose that has nothing to do with data protection must not therefore preclude the exercise of the right of access from the outset. The proposed insertion in Art. 12(5) GDPR must therefore be rejected outright in light of the case law of the CJEU.

The last inserted sentence, according to which the controller must demonstrate that the request is manifestly unfounded or that there are reasonable grounds to believe that the request is excessive, must

also be rejected from AK's point of view. The refusal of the data subject's right of access in the event of excessive exercise of the request is already possible under current law. However, according to the draft, the standard of proof for assessing whether the exercise is excessive is to be lowered, whereby mere presumption is to suffice.

The proposed amendments to Art. 12(5) GDPR must therefore be rejected in their entirety, as contrary to the Commission's announcement, they are by no means merely technical in nature, but significantly and unnecessarily restrict the right of access as the central right of data subjects.

- **Art. 13 GDPR –information to be provided where personal data are collected from the data subject**

Art. 13 GDPR regulates the obligation to provide information when collecting personal data from the data subject („privacy policy"). For data subjects, this is an important and transparent indication of what happens to their data and how they can assert their rights. For example, according to Art. 13(1) GDPR, the controller must provide information about their identity and contact details, as well as the contact details of the data protection officer, the purposes of the processing of personal data as well as the legal basis for the processing. Art. 13(2) GDPR provides for information on, among other things, the storage period and the existence of the right to request from the controller access to and the right to rectification or erasure of personal data. The controller must also provide information about any intended change of purpose in accordance with Art. 13(3) GDPR. In practice, this „privacy policy" is of great importance because it answers questions that consumers may have about when their data will be deleted, for example. According to the COM draft, Art. 13(4) GDPR is now to be reworded. Whereas previously paragraphs 1, 2 and 3 of Art. 13 GDPR did not apply if the data subject already had the information, the Commission now provides for a broader exemption from this obligation to provide information only under certain conditions.

If the personal data was used ("*in the context of a clear and circumscribed relationship*" in the course of "*exercising an activity that is not data-intensive*") and there are „*reasonable grounds to assume*" that the data subject already has certain information, namely the contact details of the controller and, where applicable, its representative, and the purpose of the processing, including the legal basis for the processing, then this information does not have to be provided according to the Commission's proposal. However, this obligation to provide information does not apply if the controller transfers the data to a third party or categories of third parties or to a third country, or if the data is used for automated decision-making, including profiling, or if the processing is likely to result in a high risk to the rights and freedoms of natural persons.

The Commission uses several vague legal terms here, which unnecessarily complicate the application of the law. For example, it is unclear what is meant by a „*clear and circumscribed relationship*" or a „*non-data-intensive activity*". The reference to the mere assumption of the controller being sufficient not to provide this information is also unclear and may in practice lead to this assumption being quickly and easily used as a pretext for not providing this information.

The exception „there are reasonable grounds to assume that the data subject already has the information" is vague and subjective, which can lead to different interpretations and applications by employers. As a result, employees may not be sufficiently informed about their data being processed about them. In the context of an employment relationship in particular, employees are often unable to understand all the personal data collected and processed by their employer, as this may come from various sources, such as personnel files, performance reviews or communication logs. Internal processes for processing personal data can be complex and opaque for employees, especially in companies without a works council, particularly if clear and comprehensive information is not provided. Employees may not have the same sources of information as employers and may therefore be disadvantaged if it is assumed that they already have the necessary information. If there is less transparency regarding the processing of personal data, employees may be less effective in exercising their rights under the GDPR (such as the right of access and the right to rectification).

For consumers, full information is also a factor in deciding whether they want to enter into a relationship with a company/controller in the first place. Regardless of this, actual practice shows that there is currently an information deficit because controllers simply do not inform their customers about data processing. This is at the expense of the data subjects, who do not know what is happening to their data. Furthermore, a complete privacy policy also helps companies to become aware of their own data processing and to take care of the right „technical and organisational measures" to protect their data. In a digital society, this is essential, as it is the only way to defend cyber attacks, etc. properly. This information should therefore always be available and disclosed to consumers and it also can lead to „competition for high data protection standards".

These key information requirements must therefore not be restricted under any circumstances. Data subjects

need the information specified in Article 13 of the GDPR, without which it is considerably more difficult for them to exercise their rights. These proposed amendments must therefore be strictly rejected.

- **Art. 22 – Automated individual decision-making, including profiling**

According to the Commission's draft, Art. 22(1) and (2) GDPR is to be replaced by a single paragraph 1. From a technical point of view, it should be noted that the reference in Art. 22(3) GDPR would then have to be corrected accordingly.

The possibility of automated decisions based on Union or Member State law (lit. b) and with the explicit consent of the data subject (lit. c) remains possible as before. However, paragraph 1 lit a, according to which the automated decision is necessary for entering into, or performance of, a contract , is supplemented in the COM draft of the GDPR in such a way that this necessity is weakened or de facto undermined insofar as an automated decision is permissible regardless of whether the decision can also be made by means other than a solely automated decision.

This addition in lit a (now drafted Art. 22(1) GDPR) represents a departure from the current general prohibition in Art. 22(1) GDPR of exclusively automated decisions with legal effect or similar significant impairment (with exceptions in the currently applicable Art. 22(2) GDPR), which, in the opinion of AK, should be rejected in any case.

Whereas currently the necessity must be assessed on the basis of the contractual objectives in each specific case and the automated decision must therefore be objectively necessary, according to the draft such a decision should also be permissible if it can be made in a non-automated manner. This opens the floodgates to automated decisions in connection with the entering into, or performance of, a contract. According to the draft, actual necessity in the sense of actual need is no longer relevant, which is to be decisively rejected from the point of view of those affected.

In future, for example, it will still be necessary to consider whether less intrusive data processing would also achieve the same purpose in an employment relationship. Data subjects must continue to have the unrestricted right not to be subject to a decision based solely on automated processing.

AK therefore clearly advocates retaining the current provision in Art. 22(1) and (2) GDPR.

- **Art. 33 GDPR – Notification of a personal data breach to the supervisory authority**

According to the Commission's proposal, Art. 33(1) GDPR is to be amended in two respects: the notification of a personal data breach is only to be made in cases of high risk (instead of risk in general) to the rights and freedoms of natural persons, and the deadline for notification has been increased from 72 hours to 96 hours.

AK opposes the proposed amendments. There is no objective justification or evidence-based necessity for increasing the risk level as a trigger for the reporting obligation or for extending the already very long deadline. The proposed changes also give rise to fears of adverse consequences for those affected, such as employees and consumers and their interest groups: they will lead to less transparency, fewer opportunities for action and co-determination – including in cooperation with the data protection authority – and make it more difficult to uncover abuses.

The obligation to report even in cases where there is a risk to the rights and freedoms of natural persons must remain in place – as stated in Recital 85 of the GDPR – a breach of personal data protection can result in physical, material or non-material damage to natural persons, which is why the controller must, as before, notify the supervisory authority of such a breach without delay (within a maximum period of 72 hours). Data protection authorities should act at an early stage and remedial measures should be taken quickly.

Furthermore, there is no reason to undermine and water down existing legal developments in this area. For example, there are guidelines on the subject or the supervisory authorities provide forms that enable low-threshold reporting. It is not clear what benefit a downward levelling in this area would have, because it is precisely a ‚data breach' report that can potentially show the supervisory authority a systematic failure, which than can be eliminated together with those responsible. In particular, this can help to identify and eliminate cybercrime or structural deficits that are detrimental to individuals and to society in a fast and proper way.

- **Art. 35 GDPR – Data protection impact assessment**

The planned harmonisation of the implementation of data protection impact assessments (DPIA) by presenting a uniform list of processing operations at EU level that require and do not require a DPIA also improves legal certainty (especially in cross-border cases) and thus also compliance by controllers. It should be noted, however, that the abolition of national lists (see regulations of the "DSB", the Austrian data protection author-

ity) could lead to specific national circumstances (existence of employee representative bodies, collective standards such as works agreements) and risks not being sufficiently taken into account in the future. The fact that the European Data Protection Board (EDPB) is responsible for drawing up these lists and proposals for the methodology for conducting the DPIA is welcomed. However, the fact that the European Commission is authorised to amend or „update" them is viewed very critically. It would be desirable for this to remain in the hands of the independent EDPB. In view of fast technological developments, the three-year review interval also appears to be too long. Ongoing monitoring and evaluation should enable new risks to be addressed more promptly.

- **Art. 88a GDPR – Processing of personal data in the terminal equipment of natural persons**

The new Articles 88a and 88b GDPR to be inserted should be read in conjunction with the addition proposed by the Commission in Article 5(3) of the e-Privacy Directive (see Article 5 of the COM proposal) and concern the so-called „cookie" regulation.

The Commission proposes to leave the processing of non-personal data in Art. 5(3) of the e-Privacy Directive and to embed the processing of personal data in the terminal equipment in a new Art. 88a of the GDPR. While a subparagraph is added to Art. 5(3) of the e-Privacy Directive, according to which the provision of Art. 5(3) of the e-Privacy Directive does not apply if the subscriber or user is a natural person and the storage or access to information constitutes or results in the processing of personal data, the proposed Articles 88a and 88b GDPR create comprehensive rules for the processing of personal data in terminal equipment of natural persons.

According to Art. 88a(1) of the Commission's proposal for the GDPR, the storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person is only allowed when that person has given his or her consent. According to paragraph 2 of the same article, the storing of personal data, or gaining of access to personal data already stored, in the terminal equipment is also permitted on the basis of Union or Member State law within the meaning of, and subject to the conditions of Article 6, to safeguard the objectives referred to in Article 23(1). This means, for example, that data processing for national security purposes is permitted if there is an appropriate legal basis.

The drafted Art. 88a(3) GDPR then regulates the permissibility of processing personal data in terminal equipment – where necessary – **without** the consent of the data subject in four listed variants: carrying out the transmission of an electronic communication over an electronic communications network (lit a); providing a service explicitly requested by the data subject (lit b); creating aggregated information about the usage of an online service to measure the audience of such a service, where it is carried out by the controller of that online service solely for its own use (lit c); maintaining or restoring the security of a service provided by the controller and requested by the data subject or the terminal equipment used for the provision of such service (lit d).

While the first two variants were already known in the application of the currently applicable Art. 5(3) of the e-Privacy Directive, the last two variants create new legal grounds for the processing of personal data in terminal equipment without the consent of the data subject.

The drafted Art. 88a(4) GDPR then creates further regulations in the event that the data subject has given consent to the storage of or access to personal data in terminal equipment: The data subject must be able to refuse consent with a „single-click button" or similar (lit a); the controller must not request renewed consent for a certain period of time during which it can lawfully rely on the consent (lit b); in the event of refusal of consent, the controller may not make a new request for consent for the same purpose for at least six months (lit c). According to Art. 88a(4), last subparagraph, the further processing of personal data also applies to the subsequent processing of personal data based on consent.

Applied to the employment relationship, this regulation allows employers to access employees' personal data on smartphones, laptops, IoT devices, etc. that they use in the course of their employment. In practice, this increases the risk that – especially in companies without workers' councils – more and more monitoring tools (and systems) will be used in future without the consent of employees, further weakening their legal position due to increased monitoring risks. Incidentally, the drafted Art. 88a(1) GDPR contradicts Art. 6 GDPR (processing on terminal equipments may also be based on legal grounds other than consent). The proposed paragraph 4 also contains wording that waters down the clear requirements for the lawfulness of processing in Art. 6 GDPR, which is bound to create legal uncertainty. It is also unclear why these new grounds for lawfulness should exist. The purposes mentioned therein can easily be achieved through Art. 6 GDPR.

The proposed provision also ignores the fact that the processing of data on terminal equipments does not take place in a closed system, but rather leads to countless third parties being able to read the personal data of data subjects because controllers, for example, use well-known website/app analysis tools or program codes or use external cloud services. These, in turn,

aggregate new data („(cross-site) tracking/profiling") and can thus generate user profiles that go far beyond the terminal equipments. This means that transparent citizens are the rule. It is incomprehensible why there should be no strict justification for this under Art. 6 of the GDPR, as the present proposal allows controllers to simply make use of the new exceptions without having to obtain consent.

The proposed provision also fails to take into account the fact that terminal equipment may be used by several people or may contain information about third parties who have no information about the processing of their data. This undermines Art. 5(2) of the GDPR, which places the responsibility for accountability on the controller. The EC's proposal implies that the natural person has the consent of these third parties for the data processing.

The current draft of Art. 88a goes far beyond the previous provision in Art. 5(3) of the e-Privacy Directive. There is no need for such a far-reaching provision in the proposed Article 88a(f) GDPR. Art. 88a(3)(c) and (d) of the draft create overly far-reaching exceptions for data processing; the further processing of personal data is also to be facilitated without necessity under Art. 88a(4), last subparagraph. The relationship to Art. 7(3) of the GDPR also remains unclear.

In any case, AK rejects this extended provision in Art. 88a GDPR; in AK's view, the current provision in Art 5(3) of the e-Privacy Directive should remain in place.

- **Art. 5(3) of the e-Privacy Directive – former „cookie" provision**

Art. 5(3) of the e-Privacy Directive previously stipulated that, in the event of storing or gaining of access to information stored in the terminal equipment, consumers must be provided with clear and comprehensive information, in particular about the purposes of the processing, and must be informed of their right to refuse such processing.

This provision is now restricted to non-personal data. In fact, however, non-personal data is now better protected than personal data in and from terminal equipment under this provision than under the newly proposed, very broadly worded Art. 88a GDPR.

From a consumers' perspective, the existing Art. 5(3) of the e-Privacy Directive should therefore remain in place. There is no need for a breakdown into Art. 88a GDPR and Art. 5(3) e-Privacy Directive; nor does it serve the purpose of legal clarity. Rather, it allows controllers to avoid having to comply with the principles of data minimisation and ‚privacy by default'. The new solution legally ‚readjusts' a system that does not work in practice and puts ongoing prevalent legal violations on a legal basis. There are already numerous court rulings dealing with the correct design of cookie banners. There is also a report on the work of the European Data Protection Board's „Cookie Banner Taskforce". All of this helps controllers to design their data processing correctly.

- **Art. 88b – Automated and machine-readable indications of data subject's choices with respect to processing of personal data in the terminal equipment of natural persons**

The proposed Art. 88b GDPR creates an obligation for controllers to give data subjects the opportunity to give their consent in an automated and machine-readable manner on their online interfaces, provided that the conditions for consent under the GDPR are met (Art. 88b(1)(a)) or to decline a request for consent and exercise the right to object under Art. 21(2) GDPR in an automated and machine-readable manner. Controllers must respect the decision made (Art. 88b(2)).

According to Art. 88b(3) of the draft, this shall not apply to controllers that are media service providers when providing a media service.

According to paragraph 4 of the draft of Article 88b, the Commission shall request a European standardisation organisation to develop standards for the interpretation of machine-readable indications of data subjects' choices. Providers of web browsers, which are not SMEs are exempt from this provision under the proposed Article 88b(6).

Although automated and machine-readable indications on decisions made by the data subject regarding the processing of personal data are generally to be welcomed, the proposed provision is vague, too broad or unclear in parts. For example, the scope of application of the provision is unclear, i.e. whether this option should only apply in the area of Art. 88a of the proposal or to all consents. It also remains unanswered whether and how it is ensured that automated and machine-readable consent constitutes an informed expression of wishes within the meaning of Art. 4(11) of the GDPR. It is also unclear whether the withdrawal of consent should also be made possible in an automated and machine-readable manner. The relationship to Art. 21(5) GDPR is also unclear. The mere respect for a decision made in Art. 88b(2) of the draft is also too vaguely worded. If the decision is to be binding, the controller must be obliged to take it into account accordingly.

This provision therefore requires further (legal) clarification or restrictions and cannot be supported in its proposed form.

- **Art. 88c GDPR – Processing in the context of the development and operation of AI**

With Art. 88c GDPR and recitals 30f, the Commission wants to base the training (development) and operation of AI with personal data on a legitimate interest, unless Union or national law explicitly requires consent. This provision does not create an independent legal basis for data processing, but is intended to apply in conjunction with Art. 6(1)(f) GDPR in the context of the development and operation of AI.

This proposal gives employers the option of relying on a legitimate interest within the meaning of Art. 6(1)(f) GDPR for the processing of personal data for the development or operation of an AI system or model, and raises considerable concerns, particularly in the context of an employment relationship. This provision and the amendment to Art. 9(2) GDPR, as well as corresponding provisions in the AI Act, are not coordinated and raise a myriad of questions.

There is a structural power imbalance between employers and employees in their relationship. Employees are often forced to disclose their data in order not to jeopardise their employment. The proposed amendment could lead to employers processing their employees' personal data to develop or operate AI systems without the data subjects having any real opportunity to object. This could significantly impair the rights and freedoms of employees. AI systems are often complex and difficult for employees and their representatives to understand. The proposed amendment could result in employees having even less control over their data and not being adequately informed about how their data is being used. AI systems based on personal data could be used to monitor employees, evaluate their performance or analyse their behaviour. This carries the risk of comprehensive control and surveillance in the workplace, which could severely restrict employees' privacy. AI models are prone to bias and discrimination, especially when trained on flawed or unbalanced data sets. The processing of employees' personal data could lead to discriminatory decisions being made. This could jeopardise equal opportunities in the workplace. Employees' participation should be ensured when introducing AI systems in the workplace, including access to data, models and decision-making logic.

Art. 88c of the draft also contains a number of vague wordings, the added value of which is highly questionable given the large number of unclear wordings. Development and operation can already be based on a legitimate interest within the meaning of Art. 6(1)(f) of the GDPR. The principle of data minimisation and the transparency obligations towards the data subject must already be complied with under current law.

In the opinion of AK, Art. 88c of the draft should therefore be deleted without replacement.

- **Supplementary provision – rights of data subjects and right to explanation**

The GDPR and the AI Act offer legal protection for AI-based decisions. The GDPR stipulates individual rights of data subjects, including the right to information regarding Article 22 GDPR, while the AI Act grants AI-specific transparency and information obligations.

The areas of application of the GDPR and the AI Act overlap, but AI systems and algorithmic decisions are not fully covered, for example, if there is neither a (high-risk) AI system under the AI Act nor fully automated decision-making under Art. 22 GDPR. In such cases, data subjects are not entitled to the corresponding legal protection options under the GDPR or the AI Act. Similarly, the distinction between automated, AI-supported and automation-assisted decision-making processes is often difficult to make in practice, which means that systems can fall into a legal „grey area".

This legal protection gap should be closed, especially if new legal bases for AI training interfere with the fundamental rights of data subjects. Since AI systems and AI-based decisions always pose a risk to the data subject's right to informational self-determination, the CJEU's case law on the right to explanation should be extended to all AI systems and algorithmic decision-making systems. A supplementary provision should oblige controllers to provide information or access to information about the logic and scope of automated or AI-based decisions.

Proposal for Article 22a:

„Persons affected by a decision taken by the controller on the basis of the output of an AI system or an algorithmic system for automated decision-making which has legal effects or similarly significantly affects them in a way which, in their opinion, adversely affects their health, their safety or their fundamental rights, shall have the right to obtain from the operator a clear and meaningful explanation of the role of the AI system in the decision-making process, the main elements of the decision taken, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject."

Artificial Intelligence Act (AI Act)

The Artificial Intelligence Act (AI Act) came into force on 1 August 2024, with most of its provisions taking effect on 2 August 2026. It has already been widely criticised by AK for its weaknesses in terms of fundamental rights protection, such as the very narrow definition of damage in the context of prohibited AI practices (see position paper from a consumer protection perspective from January 2025). The amendments to the AI Act proposed in the Digital Omnibus Package exacerbate this imbalance. What is presented as technical adjustments and measures to reduce bureaucracy turns out, on closer inspection, to be a further weakening of the regulation. The AI Act risks becoming an instrument that fails to fulfil its protective purpose even before it is fully implemented.

- **Extended exemptions for small mid-cap companies (Articles 1, 3, 11, 17, 57, 70, 95, 96, 99 AI Act) and for SMEs (Article 63 AI Act)**

The European Commission is extending the exemptions for small and medium-sized enterprises („SMEs") to larger companies. To this end, the draft AI Act introduces the definition of micro, small and medium-sized enterprises ("SMEs") in Art. 3(14a) and the definition of small mid-cap companies („SMCs") in Art. 3(14b), both taken from the Annex to Commission Recommendation (EU) 2025/1099. According to this, an SMC is defined as an enterprise with up to 749 employees, provided that either its annual turnover does not exceed EUR 150 million or its annual balance sheet total does not exceed EUR 129 million. Only when both financial thresholds are exceeded does a company fall outside the SMC definition. The combination of these criteria is intended to ensure that different business models are covered equally, such as a trading company with high turnover but low assets.

SMCs are to be granted the simplifications already provided for SMEs in the AI Act. This is in line with the proposed amendments to Art. 30(5) of the GDPR in the 4th Omnibus Package and follows the European Commission's Political Guidelines 2024-2029.

The target group for simplifications would thus be significantly expanded, with considerable disadvantages for consumers: small mid-cap companies have a particularly high share in key AI-relevant industries. In addition, around a quarter of these companies are not independent medium-sized enterprises, but subsidiaries of multinational corporations – half of which have parent companies outside the EU. The criteria for an „autonomous enterprise" defined in the annex to (EU) 2025/1099 create significant loopholes: for example, private equity investments are not taken into account unless they hold the majority of voting rights or exercise formal control. In contrast, business angels are subject to an upper limit of € 5 million under point 3.4 of the annex to Recommendation (EU) 2025/1099. This means that a start-up with 300 employees, € 5 million in business angel financing and a professional management team is treated in the same way as a traditional family business with 30 employees and no external financing – despite vastly different resources and capabilities. While the targeted relief for SMEs in the AI Act represented a balance between the limited resources of small businesses and the level of protection, the extension to medium-sized companies effectively negates this advantage.

In the AI Act, the extended simplifications for SMCs mainly concerns two key provisions: technical documentation under Art. 11 and quality management systems under Art. 17 of the AI Act. Art. 11(1) of the AI Act currently allows for the simplified presentation of technical documentation under Annex IV for SMEs, including newly established companies. Art. 17(2) of the AI Act stipulates that the implementation of a quality management system as defined in more detail in paragraph 1 should be proportionate to the size of the supplier's organisation.

The proposal to extend the simplifications intended for SMEs and start-ups to SMCs must be rejected for several reasons: The AI Act, as product safety legislation for artificial intelligence, stipulates requirements for artificial intelligence according to the risk of the AI system. The simplifications proposed by the Commission in the AI Act for SMCs lack any objective justification, as the AI Act is concerned with risk reduction and harm prevention, based on the risk posed by the AI system, not on company size. The proposed simplifications are therefore unacceptable from the point of view of those affected. Articles 11 and 17 of the AI Act are essential quality assurance instruments for high-risk AI systems that determine creditworthiness, employment opportunities, social security entitlements or biometric identification. From the AK's point of view, a functioning quality management system and complete technical documentation are particularly critical in these contexts.

The proportionality clause in Art. 17(2) of the AI Act and the simplified documentation under Art. 11(1), second subparagraph, of the AI Act presuppose that smaller organisations do not have the structural capacities of large corporations. However, SMCs typically have hundreds of employees and dedicated compliance departments – equating them with SMEs and start-ups therefore lacks any factual basis.

The proposed amendment to Art. 99 of the AI Act, according to which the interests of SMCs must now also be taken into account with regard to sanctions, should also be rejected in the opinion of the AK.

The proposed amendment to Art. 63(1) of the AI Act, according to which SMEs in general, rather than micro-enterprises, would benefit from the exemptions stipulated here, is also relevant in this context. In the absence of objective justification, the AK is opposed to such an extension to SMEs.

- **Art. 4 AI Act – AI literacy**

Art. 4 of the AI Act already takes a non-binding approach to AI literacy in its current version and merely obliges companies to ensure „to their best extent" that their staff has a „sufficient level" of AI literacy. Art. 4 of the AI Act is a prerequisite for compliance with Art. 14 of the AI Act, which regulates human oversight. Without a sufficient level of AI literacy, the human oversight required for high-risk AI cannot be ensured.

Art. 4 of the AI Act is also important because it is one of the few obligations for non-high-risk AI systems in the AI Act.

However, the proposed amendment intends to downgrade this already minimal obligation to a mere recommendation: the Commission and the Member States would merely „encourage" providers and deployers to provide AI literacy, rather than requiring it. This proposed vague and non-binding wording not only means the abolition of the obligation for providers and deployers to ensure AI literacy, but also that AI literacy will play no role at all in the introduction and use of AI. This is problematic both from a societal perspective and in terms of competitiveness: for companies, AI literacy is the basis for minimising risks, on the one hand with regard to the potentially negative effects on the health, safety and fundamental rights of employees, for example, and on the other hand with regard to liability or misuse of AI systems. Furthermore, AI literacy is the basis for the productive use of AI. The de facto abolition of this obligation therefore also contradicts the strategic objectives of the EU (e.g. Apply AI Strategy). From a societal perspective, AI literacy is the basis for collective control and the preservation of democratic values. Instead of abolishing the obligation, the duties of the Commission and the Member States to promote AI literacy should be expanded.

This proposal should therefore be rejected from the perspective of those affected. For product safety legislation such as the AI Act, ensuring that providers are competent in using a system should be the absolute minimum – not only for high-risk AI systems. Art. 4 of the AI Act has been applicable since February 2025, but no documented enforcement cases are known to date. In practice, however, violations of the literacy obligation will likely only become apparent when high-risk systems fail and investigations identify insufficient AI literacy as the cause. At this point, the difference between „ensuring literacy" and „encouraging the provision of literacy" will be crucial for liability and responsibility.

Competent employees who are well prepared for the new challenges in the company and are involved in planning digitalisation facilitate the introduction and application of AI as well as the redesign of internal processes and workflows. The necessary AI literacy arises directly from the specific company or organisational context and the AI technologies used there. Responsibility for the implementation of AI systems and their intended use lies with the companies themselves and is also determined by their strategic orientation. Consequently, the development of the necessary AI literacy must also take place within the companies themselves. Transferring these tasks to the Commission or its Member States would not be effective and would defeat the purpose of the regulation. Therefore, the argument of „additional compliance burden" is not convincing. Companies themselves benefit from improved work processes, support from AI technologies, increased security in dealing with AI, and an understanding of their own rights and obligations in the context of AI applications.

- **Art. 4a AI Act – Processing of special categories of personal data for bias detection and mitigation**

The introduction of a new Art. 4a is planned, which would allow the processing of special categories of personal data for the purpose of detecting and correcting bias. While the proposed Art. 4a(1) AI Act largely corresponds to Art. 10(5) AI Act, Art. 4a(2) now extends the permission to use special categories of personal data to providers and deployers of all AI systems and models and deployers of high-risk AI systems, insofar as this is necessary for the specified purposes.

This represents a massive extension of the exception for the processing of special categories of personal data, which was originally only intended for high-risk AI systems, and should be rejected in any case from the AK's point of view. Art. 10(5) of the AI Act should remain unchanged.

- **Deletion of the registration obligation for AI systems under Annex III that are not high-risk AI systems from a business perspective (Article 6(4), Article 49(2) of the AI Act)**

The Commission proposes to remove the registration requirement under Art. 49(2) of the AI Act. Under Art. 49(2) of the AI Act, providers of a high-risk AI system who conclude that it is not high-risk under Art. 6(3) of the AI Act are required to register that system in an EU database referred to in Art. 71 of the AI Act before the AI system is placed on the market or put into service. The registration requirement in Art. 49(2) of the AI Act was introduced as a protective measure to ensure

transparency and public accountability for companies that wish to exempt the AI system they have developed from the high-risk classification. The registration process involves minimal bureaucracy, but is highly relevant from the perspective of those affected. This is because the information given by a provider enables external verification of exemption decisions.

The proposal to remove these registration requirements should therefore be rejected from the AK's point of view. Providers would retain the option of avoiding high-risk classification through self-assessment without these decisions being publicly documented or subject to supervision. This creates a loophole in the AI Act that is particularly worrying, as AI systems, by definition, initially meet the criteria for high-risk classification based on their intended purpose and context of use, in accordance with Art. 6(3) of the AI Act.

Furthermore, as the current handling of the DPIA (Art. 35 GDPR) shows, the removal of the registration requirement could lead to the exception in Art. 6(3) of the AI Act being interpreted arbitrarily by many organisations, or to documentation not being carried out in practice. This would put organisations that work in a legally compliant and conscientious manner, as well as the individuals affected by such a system, at a disadvantage.

- **Art. 43(3) AI Act – Conformity assessment**

Art. 43 of the AI Act deals with the conformity assessment of high-risk AI systems, with paragraph 3 regulating high-risk AI systems falling under Annex I, Section A. According to this, providers must meet the requirements set out in the listed regulations, whereby the requirements of the AI Act relevant to them must be incorporated into the assessment. The body notified in accordance with these listed legal acts is authorised to carry out this assessment, whereby, according to the Commission's proposal in Art. 43(3), second subparagraph, of the AI Act, it must apply or designation as the competent body no later than 18 months after the AI Act becomes applicable.

If a high-risk AI system falls under both a Union harmonisation measure in Section A of Annex I and one of the categories in Annex III, the provider must comply with the relevant assessment procedure in the specific Union legislation (proposed Art. 43(3), last subparagraph, of the AI Act).

It is initially unclear why the bodies already responsible for conformity assessment under the specific Union harmonisation provisions must now also apply to become competent bodies under the AI Act and what happens if they fail to do so. It also remains unclear what will happen in the period between the application of the AI Act (i.e. 2 August 2026 according to Art. 113 of the AI Act) and the application to become a competent body under the AI Act. Recital 8 of the Commission's proposal, which is relevant here, does not provide any clarity in this regard either. AK therefore suggests that the open issues mentioned above be explained, for example in a recital.

- **Art. 50(7) AI Act – Transparency obligations for providers and deployers of certain AI systems; deletion of implementing acts**

According to Art. 50(7) of the AI Act, the development of practical guidelines for the effective implementation of the obligations regarding the detection and labelling of artificially generated or manipulated content should be promoted and facilitated by the AI Office. The Commission may adopt implementing acts to approve these practical guidelines, thereby giving them general validity.

According to the proposal, this possibility for the Commission to adopt implementing acts to approve these practical guidelines is now to be deleted. From a consumer perspective, this is to be rejected and in no way serves legal certainty. Without implementing acts, the guidelines remain voluntary with no legally enforceable consequences in the event of non-compliance, which is to be rejected in any case.

- **Art. 57(3a) Creation of an AI regulatory sandbox at EU level for AI systems pursuant to Art. 75(1)**

The proposal is expressly welcomed, particularly as it eliminates the need for specific legal bases for AI training in the GDPR (proposed amendments to Art. 9(2) GDPR and Art. 88c GDPR). Under the supervision of the competent authority, high-risk AI systems and, with the creation of this additional AI regulatory sandbox, AI systems subject to Article 75 of the AI Regulation can already be trained without having to restrict data protection in general.

- **Art. 60a AI Act – Testing of high-risk AI systems covered by Union harmonisation legislation listed in Section B of Annex I in real-world conditions outside AI regulatory sandboxes**

The proposed Art. 60a of the AI Act is intended to enable easier testing under real-world conditions for products listed in Section B of Annex I compared to Art. 60 of the AI Act. This affects AI systems related to means of transport such as motor vehicles, railway systems or marine equipment.

From the AK's point of view, the need for such simplified testing under real-world conditions for this group of AI systems is questionable. It would be better to continue applying Art. 60 of the AI Act as before, thereby ensuring that all the protective measures standardised therein are complied with.

- **Art. 72 AI Act – Post-market monitoring by providers and post-market monitoring plan for high-risk AI systems**

According to Art. 72 of the AI Act, providers must establish and document a monitoring system after placing the high-risk AI system on the market. Art. 72(3) of the AI Act, which prescribes a post-market monitoring plan, is now to be amended in line with the Commission's proposal so that the Commission only has to draw up guidelines for such a post-market monitoring plan and no longer has to adopt an implementing act in this regard, as is currently the case.

AK is against mere guidelines; the current provision of Art. 72(3) of the AI Act should remain unchanged, thereby ensuring binding legal acts (instead of voluntary guidelines).

- **Art. 75 AI Act – Market surveillance and control of AI systems in the Union market**

According to the proposal, Art. 75 of the AI Act is to be given a new heading: „Market surveillance and control of AI systems and mutual assistance" instead of the previous heading as mentioned above.

In addition to the heading, the provision of Art. 75(1) will also be amended and supplemented by paragraphs 1a to 1c. According to the proposed Article 75(1) of the AI Act, the AI Office shall also be responsible for monitoring and enforcing the obligations of this Regulation in relation to AI systems that are part of a designated very large online platform or very large online search engine within the meaning of the DSA. This is consistent, especially since the EC also has powers regarding VLOPs and VLOSEs under the Digital Services Act (DSA).

The further proposed paragraphs 1a to 1c contain implementing acts for the design of the relevant powers of the AI Office (paragraph 1a), a reference to the Market Surveillance Regulation (paragraph 1b) and an obligation on the Commission to carry out conformity assessments for high-risk AI systems before they are placed on the market, whereby this assessment may also be outsourced to notified bodies (paragraph 1c).

AK welcomes these changes, as they strengthen control over large AI systems and AI model providers in particular.

Art. 77 AI Act – Powers of the authorities protecting fundamental rights

First, the Commission proposes an amendment to the heading, which would also include cooperation with market surveillance authorities in the heading. Furthermore, the scope of application of national authorities and bodies is no longer limited to high-risk AI systems as defined in Annex III. The removal of this reference to Annex III is welcomed, as it means that, for example, the Machinery Regulation (which is relevant to the health and safety of workers) is also covered. The addition of information (in addition to documentation, as was previously the case) to which access must now be granted is also welcomed by AK.

The proposal to obtain information and documentation via the competent market surveillance authority is expected to facilitate the tasks of Art. 77 bodies, as it entrusts a central body with the procurement of documentation (i.e. the documentation does not have to be requested from individual employers) and cooperation between Art. 77 bodies and the competent market surveillance authority is facilitated.

- **Art. 111 AI Act – AI systems already placed on the market or put into service and AI models already placed on the market for general purpose**

- **Art. 113 AI Act – Entry into force and application**

According to the Commission's proposal, Art. 111(2) of the AI Act should be amended and a new paragraph 4 added.

Art. 111(2) of the AI Act governs the application of the AI Act to deployers of high-risk AI systems that were already placed on the market or put into service before 2 August 2026. According to the EC's proposal, a specific date (2 August 2026) is no longer specified here, but reference is made to the date of application of Chapter III and the corresponding obligations under Art. 113.

According to the proposal, a new paragraph 4 is to be added to Art. 111 of the AI Act, according to which providers of AI systems, including those for general purpose, that generate synthetic audio, image, video or text content and are placed on the market before 2 August 2026 must comply with the requirements of Art. 50(2) by 2 February 2027.

However, the operators and deployers of such AI systems are not covered by this provision and must therefore already comply with it by 2 August 2026. There is no justification for such a distinction, which is why this additional paragraph should be deleted without replacement.

Article 113 of the AI Act is to be amended in such a way that, following a decision by the Commission that adequate measures are in place to support compliance with the provisions of Chapter III, apply six months after that decision in relation to high-risk AI systems under Art. 6(2) and Annex III, or 12 months after that decision in relation to high-risk AI systems under Art. 6(1) and Annex I, or, in the absence of such a decision, from 2 December 2027 or 2 August 2028, respectively.

This postpones the date of application from 2 August 2026 to 2 December 2027 or 2 August 2028, which AK rejects in any case. The postponement creates further legal uncertainty and is therefore firmly rejected.

After reviewing this proposal, it is also unclear when Article 6(1) of the AI Act is to apply. In Article 113(c) of the AI Act, which is not to be amended according to the draft, the date of application of Article 6(1) is set at 2 August 2027. According to the newly proposed lit d second subparagraph (ii) of Article 113, the date of application is to be set at 2 August 2028 at the latest, which, as explained above, is to be rejected by AK.

Contact Us!

In Vienna:

Jasmin Reininger
T +43 (1) 501 65 12801
jasmin.reininger@akwien.at

Louise Beltzung
T +43 (1) 501 65 12324
louise.beltzung@akwien.at

Jakob Kalina
T +43 (1) 501 65 13720
jakob.kalina@akwien.at

Austrian Federal Chamber of Labour
Prinz-Eugen-Straße 20-22
1040 Wien, Österreich
T +43 (0) 1 501 65-0

www.arbeiterkammer.at

In Brussels:

Alice Wagner
T +32 (2) 230 62 54
alice.wagner@akeuropa.eu

AK EUROPA
Permanent Representation of Austria to the EU
Avenue de Cortenbergh 30
1040 Brussels, Belgium
T +32 (0) 2 230 62 54

www.akeuropa.eu

About Us

The Austrian Federal Chamber of Labour (AK) is by law representing the interests of about 3.8 million employees and consumers in Austria. It acts for the interests of its members in fields of social-, educational-, economical-, and consumer issues both on the national and on the EU-level in Brussels. Furthermore, the Austrian Federal Chamber of Labour is a part of the Austrian social partnership. The Austrian Federal Chamber of Labour is registered at the EU Transparency Register under the number 23869471911-54.

The main objectives of the 1991 established AK EUROPA Office in Brussels are the representation of AK vis-à-vis the European Institutions and interest groups, the monitoring of EU policies and to transfer relevant Information from Brussels to Austria, as well as to lobby the in Austria developed expertise and positions of the Austrian Federal Chamber of Labour in Brussels.