Submission to the Public Consultation on the

Digital Omnibus on AI COM(2025) 836

Prighter Group

Vienna 13.03.2026

About Prighter and This Feedback

Prighter is a group of companies acting as the representative for over 2,000 companies under EU and non-EU data protection, digital governance and AI regulations and providing software to simplify the compliance obligations stemming from these frameworks.

In response to the EU Commission's open consultation on its Digital Omnibus proposal, Prighter has prepared this submission by distributing a questionnaire to our clients asking for feedback on the European Commission's ("**Commission**") proposal for the Digital Omnibus[1]. Where we had sufficient data the clients' answers went into our position as outlined below.

The main criteria covered by the questionnaire and for the assessment of the proposed changes are the Digital Omnibus' main objectives of simplifying the digital rulebook and easing the administrative burden for companies, especially for SMEs and for the new category of SMCs. Our assessment is driven by the practical applicability of the digital rulebook and the proposed changes to it.

Our feedback is split into two submissions, one for the Digital Omnibus on AI COM(2025) 836, and one for the Digital Omnibus COM(2025) 837. Attached to this submission as Annex I is the feedback on the Digital Omnibus. The structure of our feedback follows the structure of the Digital Omnibus. Feedback is only provided where we recommend changes to the Commission's proposal.

Executive Summary

Prighter welcomes the Commission's Digital Omnibus proposal as a meaningful step towards simplifying the AI regulatory framework and reducing administrative burdens across the Single Market. Drawing upon feedback from our clients, including SMEs and non-EU-providers, Prighter's assessment is grounded in the practical operability of the proposed changes.

While the objective of simplifying regulatory requirements is welcome, certain changes risk weakening important governance safeguards and creating legal uncertainty. In particular, the proposed amendments to AI literacy obligations, the deletion of registration requirements for certain high-risk AI systems, and the lack of clarity regarding implementation timelines may undermine transparency and effective compliance.

Furthermore, introducing an AI-specific clarification of the legitimate interest legal basis risks departing from the technology-neutral approach of the GDPR. We therefore recommend targeted adjustments that preserve transparency, legal certainty, and risk-based governance framework of the AI Act while still supporting simplification.

[1] Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/1679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854, and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus).

1. General Remarks

The Digital Omnibus proposes a series of amendments to the AI Act intended to simplify compliance, reduce administrative burdens, and support the operalisation of AI governance across the European Union. While these changes are broadly welcome, care must be taken to ensure that simplification does not come at the expense of fundamental safeguards and legal certainty. Clear guidance, proportionate obligations, and predictable timelines are essential to maintain trust, facilitate responsible AI deployment, and support innovation across the Single Market.

2. Proposed changes to the AI Act

2.1. AI Literacy:

The objective of ensuring a sufficient level of AI literacy among organisations developing and deploying AI systems is an important element of the AI Act's governance framework. Promoting a basic understanding of AI systems, their capabilities and limitations, and their potential impact on individuals is essential for the responsible use of such technologies. This is reflected in Recital 82 of the AI Act, which recognises that AI literacy is a prerequisite for effective human oversight, particularly in the context of high-risk AI systems.

The proposed amendment to Article 4 would change the provision from a direct obligation for providers and deployers to take measures ensuring AI literacy, to a framework in which the Commission and Member States merely encourage such measures.

While the intention to simplify compliance requirements is understandable, this change may significantly reduce the incentive for organisations to develop structured AI literacy programmes.

In practice, AI literacy supports several key objectives of the AI Act, including:

- enabling staff to correctly interpret and use AI systems,
- supporting effective human oversight,
- reducing operational risks and unintended misuse of AI systems, and
- fostering a culture of responsible and trustworthy AI deployment.

For many organisations, particularly those integrating AI into existing digital services, AI literacy represents a practical and proportionate governance tool that helps operationalise broader AI Act obligations.

Rather than fully replacing the obligation with a non-binding encouragement, it may be preferable to maintain a principle-based obligation while providing greater flexibility in its implementation. For example, the provision could clarify that organisations may adopt risk-based and proportionate measures, taking into account the nature, scale, and context of the AI systems they develop or deploy.

Such an approach would preserve the importance of AI literacy as a foundational governance mechanism, while still supporting the broader objective of reducing unnecessary administrative burdens.

Recommendations:

- **Maintain a binding minimum requirement**: Reintroduce a clear obligation for providers and deployers to ensure that their staff and other users handling AI systems achieve a sufficient level of AI literacy, at least for roles critical to the operation, deployment, and oversight of AI systems.
- **Encourage practical guidance and standards**: Provide guidance or standards for AI literacy that specify training modules, assessment methods, or certification, ensuring a consistent baseline across the Union.
- **Risk-based tailoring**: Ensure that the level and depth of AI literacy required are proportionate to the complexity and risk profile of the AI systems being used, so that higher-risk systems trigger more comprehensive training.

  This approach balances the need for practical feasibility for providers (especially SMEs) with the protection of individuals and society by ensuring that staff and deployers are sufficiently informed about the AI systems they operate, thereby reducing risks of misuse, errors, or bias.

2.2. High-risk AI providers' register assessments

The Digital Omnibus proposes to delete certain registration obligations for high-risk AI systems listed under Annex III in the EU database. While reducing administrative burdens is a legitimate objective, the deletion of registration obligations raises concerns regarding transparency and accountability that warrant careful consideration.

The EU database serves an important function beyond administrative formality. It enables authorities, deployers, and affected individuals to identify which systems are in use and in which contexts - a function that is particularly relevant for systems with a significant impact on individuals' rights, such as those used in employment, education, or access to essential services. While simplification of registration procedures is welcome, outright deletion risks creating an accountability gap.

In addition, the EU database can serve as a valuable transparency tool for other market actors, including organisations considering the deployment of AI systems. Accessible information about registered high-risk AI systems can support companies in assessing potential vendors and understanding regulatory classifications. Maintaining a certain level of registration therefore not only supports regulatory oversight, but can also contribute to market transparency and informed decision-making by deployers and other stakeholders within the AI ecosystem.

For these reasons, rather than removing registration obligations entirely, it may be preferable to simplify or streamline the registration process, ensuring that transparency objectives are preserved while reducing unnecessary administrative burdens.

Recommendations:

Rather than deleting registration obligations entirely, the co-legislators should consider streamlining the registration process while preserving its core transparency function.

2.3. Legal certainty regarding implementation timelines

The proposed amendments to Articles 111 and 113 introduce transitional rules for high-risk AI systems and general-purpose AI models already placed on the market before the application of Chapter III. Under Article 111(2), these systems are only subject to the obligations of Chapter III if they undergo significant design changes, while providers and deployers of high-risk AI systems intended for public authorities must comply by 2 August 2030. Article 113 links the enforcement of high-risk obligations to the availability of necessary standards, measures, and implementing acts, but the proposed text leaves considerable uncertainty about when postponed obligations will take effect.

This creates potential legal and operational uncertainty for providers and deployers: companies cannot plan compliance investments effectively when enforcement dates are linked to processes with no predictable endpoint. Moreover, the combination of Articles 111 and 113 may unintentionally create a gap between postponement and the actual applicability of high-risk rules, leaving both authorities and businesses unsure of their obligations.

Recommendations:
Clarify the timelines by:

- Explicitly linking the application of postponed obligations to the formal adoption of relevant standard, guidelines, or implementing acts, with clear predictable triggers.
- Providing a fixed grace period of at least 12 months from the adoption of these measures for both existing and newly-placed high-risk AI systems, ensuring that providers and deployers have sufficient time to prepare and implement compliance measures.
- Maintaining proportionality by applying these timelines consistently, without creating separate transitional rules for subsets of AI systems, to avoid confusion and uneven application across the EU market.

This approach would provide legal certainty, operational predictability, and a realistic timeframe for compliance while preserving the effectiveness of the AI Act's high-risk safeguards.

2.4. Legitimate interest legal basis for AI processing

The proposal aims to clarify that the development and operation of AI systems may rely on legitimate interests as a legal basis for processing personal data. While the objective of increasing legal certainty for organisations has wide spread support, it is not evident that an additional clarification is necessary.

Article 6(1)(f) GDPR already provides a well-established legal basis for processing based on legitimate interests, subject to the balancing test between the interests of the controller and the fundamental rights and freedoms of data subjects. Many AI-related processing activities can already rely on this provision where the applicable conditions are met.

Introducing a specific reference to AI processing may risk departing from the technology-neutral approach of the GDPR, which deliberately regulates personal data processing independently of the technologies used. This principle is expressly reflected in Recital 15 of

the GDPR, which clarifies that data protection rules apply regardless of the technologies used for processing, and should not be undermined by technology-specific carve-outs. It could also create the perception that AI processing benefits from a privileged legal pathway compared to other forms of data processing.

Recommendations:
While some practical clarification on the application of Article 6(1)(f) GDPR to AI processing may be useful, legislative amendment is not the appropriate vehicle. Introducing AI-specific wording risks departing from the GDPR's technology-neutral framework, as reflected in Recital 15 GDPR, and may create the unintended perception that AI processing benefits from a lowered threshold compared to other forms of data processing. As noted by other stakeholders in this process, poorly drafted AI-specific provisions risk creating interpretive uncertainty rather than resolving it.

We therefore recommend that the Commission withdraws the proposed legislative amendment and instead issue dedicated guidance clarifying how the existing balancing test under Article 6(1)(f) GDPR applies in the context of AI development and operation, without altering the underlying legislative framework.

Annex I

Submission to the Public Consultation on the

Digital Omnibus – COM(2025) 837

Executive Summary

Prighter welcomes the European Commission's initiative to simplify the digital regulatory framework and reduce administrative burdens, particularly for SMEs and the newly introduced category of small mid-cap companies (SMCs). Our submission focuses on the practical applicability of the proposed changes.

On the Data Act, we support the consolidation of data-sharing rules but caution that merging additional roles from the Data Governance Act risks compounding existing confusion about the Data Act's scope. On switching between data processing services, we welcome relief for SMEs but warn that maintaining parallel regimes depending on the date of the clients' contracts creates operational complexity that undermines the simplification objective.

On the GDPR, we strongly oppose the proposed amendment to the definition of personal data, which we consider more complex than the current framework. We support streamlined rules on data subject access requests but caution that allowing companies to reject requests without providing reasons risks eroding data subject trust. On the privacy notice exemption, we call for clear, objective, and workable criteria tied to company size or industry sector.

On incident reporting, we strongly support a single point of entry for notifications but recommend extending its scope explicitly to non-EU companies, harmonising reporting deadlines across all regulatory frameworks, and standardising communication channels with supervisory authorities.

Across all areas, our overriding recommendation is to prioritise full harmonisation, legal certainty, and global consistency — avoiding changes that fragment the EU's role as a global regulatory gold standard.

1. General Remarks

The EU Commission's objective to simplify the digital rulebook is welcomed and supported by all stakeholders. However, a distinction must be drawn between established rules and those which are newly introduced. The data from the Questionnaire shows that our clients are operating in multiple jurisdictions and across Member States, which seems to be the nature of a modern, digital business model in general, regardless of whether big or small. Furthermore, the vast majority of companies responding to the Questionnaire have a unified compliance project in place for all countries in which they operate and deal with outliers where necessary. Simplification in this case means:

- **Striving for full harmonisation of the digital rulebook in all EU Member States and reducing opening clauses and gold-plating**:
  Harmonisation is not only essential in removing barriers in the single market but also for companies' internal processes. Deviations are costly and complex, for example, implementing an age verification process with different age limits and requirements in Member States has proven to be very complicated.

- **Having a global gold standard:**
  The GDPR has been very successful as a European export. Many legislators have adopted key concepts of the GDPR in local data protection regulations. This makes it easier for companies with cross-border operations to streamline their internal processes.

  A recent example of this was the Data Use and Access Bill in the United Kingdom. After an initial draft, which deviated from the GDPR, the United Kingdom eventually decided to reduce the deviations to a minimum, especially because UK companies had already established processes to comply with the existing legal framework and because any deviation would not have had any easing effect for UK businesses which are also active in the EU. To the contrary, the deviation would have increased complexity, as companies with cross-border activities would have been forced to change their existing processes to comply with two different sets of rules.

  The fact that core principles of the GDPR have been mirrored by major EU trade partners makes it easier for companies in the EU to expand beyond that market while still relying on the GDPR as the gold standard. As with UK companies previously, any deviation from the UK GDPR, or other countries following the same principles, makes compliance for EU companies more difficult. This is why changing core principles, like the definition of personal data, should be avoided, especially because such changes do not result in simplification when companies are active in other regions where data protection laws conform to original GDPR concepts.

- **Predictability and Continuity:**
  The answers to the Questionnaire show that compliance with the GDPR has matured, while compliance with other parts of the Data Acquis and the AI Act is still at a very early stage, with limited awareness.

  This means that for the GDPR companies have established processes and there is a market of consultants and software providers to enable compliance. Changes to the legal framework will require additional investment from all stakeholders and therefore need to be treated with more caution than changes to the rest of the Data Acquis and the AI Act, which may not have the same impact.

2. Proposed Changes to the Data Act

2.1. Consolidation

The consolidation of rules for data sharing is welcomed and reduces overlap and confusion. Other than the Commission, we found in our discussions and the Questionnaire that the familiarity with the Free Flow of Non-Personal Data Regulation (FFDR), the Open Data Directive and the Data Governance Act ranges from very low to non-existent. Familiarity with the Data Act is slightly higher, however knowledge remains vague.

The basic issue with the Data Act, from what we heard from our clients, is that companies are unclear as to whether Chapters in the Data Act apply to them. The different roles in the Data Act which are subject to different Chapters are still confusing to companies. Introducing two additional roles in the Data Act by moving the rules on data intermediation services provider and data altruism organisation from the Data Governance Act into the Data Act will only compound this issue.

Furthermore, turning the mandatory regime, which has already been proven to be ineffective, into a voluntary scheme may make the rules on data intermediation services providers and data altruism organisations irrelevant.

Recommendations:
We recommend assessing the practical relevance of the rules on data intermediation services and data altruism. If the relevance is expected to stay low or even decrease, we recommend repealing also the rules on data intermediation services and data altruism and not moving them into the Data Act.

2.2. Switching between data processing services

The Digital Omnibus suggests a lighter regime for data processing services that are custom-made if the provision of such services is based on a contract concluded before the Data Act became applicable (12 September 2025). Furthermore, an exemption is introduced for small and medium-sized enterprises (SMEs) as well as small mid-cap companies (SMCs), again if applicable for contracts concluded before 12 September 2025. These providers can also include early-termination penalties in fixed-term contracts.

While the lighter regime for SMEs and SMCs would be welcomed, the benefits of the exemption are outweighed by the administrative burden to maintain two regimes in parallel depending on when the contract was concluded.

Furthermore, the Data Act's concept of reducing lock-in and removing barriers to switch providers jeopardises a very common pricing model for data processing services. One type of data processing service is delivered through Software as a Service (SaaS) providers, who typically use a subscription model with fixed terms where longer commitments are awarded with discounts (e.g. 10% discount for annual contracts; 15% discount for bi-annual contracts). The current rules allow companies to enter into long-term contracts in return for better pricing, which can then be terminated at short notice before the renewal date. To avoid such imbalance, data processing services should be able to charge the difference between the discounted long-term pricing and the regular price when a client switches providers and terminates the contract at short notice.

Recommendations:
We recommend not limiting the exemption for custom-made data processing services and for SMEs and SMCs to contracts concluded before 12 September 2025, but providing these exemptions for all contracts no matter when concluded.
Furthermore, we recommend allowing all data processing services to charge for the difference between a long-term and a short-term contract when clients want to switch before the end of a long-term contract.

3. Proposed Changes to the GDPR

3.1. Definition of "Personal Data"

The Commission proposes an amendment to the definition of "personal data" introducing a subjective criterion to the definition qualifying data as personal only if an organisation has means reasonably likely to be used to identify the natural person. The fact that another organisation may be able to identify the individual would not, by itself, make the information personal data for the first organisation. According to the Commission's reasoning this amendment reflects the recent case-law of the CJEU, especially C-413/23P EDPS v SRB ("**SRB-Case**").

The classification of data as personal is the first step in the assessment of the applicability of the GDPR. If qualified as personal, the processing of such data triggers all obligations under the GDPR, for companies the very basic definition of the role as controller, joint controller, or processor. Related to the role are obligations to govern the data processing between companies and in the chain of suppliers through joint controller agreements or data processing addendums ("**DPA**") as well as the question of international data transfer. In a B2B relationship both parties are liable to put the necessary documents in place.

The proposed change of the definition of personal data would have the effect that every company needs to decide on a case-by-case basis which of their partners have means reasonably likely to be used to identify the natural person. A typical SaaS company has thousands of B2B clients, and under the proposed definition, would need to assess individual clients based on their ability to re-identify a person, rather than taking a one-size-fits-all approach. Such an assessment depends on the accuracy of the information given by B2B partners which makes a company and its liability risk dependent on the proper understanding and quality of internal assessment of another organisation. At Prighter, we interact with companies around the world daily and our work involves constantly explaining the basics of the GDPR, especially the qualification of an organisation as a controller or processor. We doubt that the proposed definition, which is more complex than the existing one, will lead to simplification, greater legal certainty, or a reduction of administrative burden.

Prighter urges the Commission to withdraw the proposed amendment to the definition of personal data. Where simplification is genuinely sought, it should be pursued through guidance and supervisory practice rather than by amending the foundational scope of the GDPR.

Moreover, the "means reasonably likely to be used to identify the natural person" are subject to technical advancements and therefore change over time. As proven by researchers from ETH Zurich and Anthropic "large language models can be used to perform at-scale deanonymization."[2]

From a legal point of view, the EDPB together with the EDPS highlighted in their Joint Opinion 2/2026 that the proposed amendments go beyond the recent case law. We share this opinion and would like to emphasise that the facts of the SRB-Case were very specific and, in our opinion, do not allow for generalisation. Building on the publicly available arguments, we would like to emphasise that subject to the SRB-Case were two separate controllers sharing very specific data, whereas the amendments to the definition would be applicable irrespective of the roles of the involved parties. In a chain of controllers and processors, any processor would fall out of the scope of the GDPR if provided with pseudonymised data which allows for a data outsourcing strategy designed to avoid the applicability and therefore the protection of the GDPR. In case of joint controllers there is also case law conflicting with the proposed amendment of the definition of personal data.[3]

Recommendations:
For the reasons mentioned above we recommend to keep the current definition of "personal data" and not change it as proposed in the Digital Omnibus.

[2] *Lermen, Paleka, Swanson, Aerni, Carlini, Tramèr*, Large-scale online deanonymization with LLMs, arXiv 2602.16800, available under https://arxiv.org/pdf/2602.16800.
[3] C-604/22 IAB Europe

3.2. Artificial Intelligence: Legitimate Interest

Please see our feedback on the proposed changes for the use of legitimate interest in the context of AI in our submission on the Digital Omnibus on AI.

3.3. Data Subject Rights: Access

The Commission is proposing an amendment to Art 12 (5) of the GDPR clarifying that information provided to data subjects under Art 13 and 14 and actions under Art 15-22 should generally be free of charge. Controllers may, however, charge a reasonable fee or refuse to act if requests are manifestly unfounded, excessive, repetitive, or intended for purposes other than data protection. In such cases, the controller would need to demonstrate that a request is manifestly unfounded or that there are reasonable grounds to consider it excessive. The burden of proof has not been extended to abusive requests.

In our role as representative, we are addressee for data subjects and as such have seen many abusive requests. However, abusive requests are still a small percentage, and the vast majority of requests are legitimate. On the other hand, we have seen companies unable or unwilling to respond to any kind of requests.

The right to access serves data subjects with transparency and data ownership. It is fundamental to build trust between a company and its customers. Refusing to handle a request may lead to an increased number of complaints with authorities, because abusive requests often are a result of tensions or an escalation between the involved parties. Not handling such requests may increase the tensions and drive a data subject to lodge a complaint.

Recommendations:
Because of the reasons mentioned above, we recommend not amending the exemption for handling access requests.

3.4. Information Obligation – Privacy Notice

The Commission is considering an amendment to clarify that information obligations may not apply if the data is collected in a clear, limited context, the processing is not data-intensive, and the data subject is likely to already have the information. The exception would not apply if the data were shared, transferred internationally, used for automated decision-making or profiling, or is likely to pose a high risk to the data subject.

Companies which we have consulted all share or transfer data internationally. This is particularly true for SMEs, which typically lack their own technical infrastructure and rely on external service providers, often located outside the EU.

The proposed wording for the amendment of Art 13 GDPR also suggests that the exemption depends on the individual relationship between a data subject or a group of data subjects and

a company and the information the data subject has already which both requires a case-by-case analysis. For companies, such individual requirements are impossible to operationalise and build a reliable process around it and therefore results in more complexity instead of simplification.

The proposed exemption offers little practical benefit and fails to simplify compliance. To make it effective, the Commission should define clear, objective criteria—such as company size (e.g., businesses with fewer than 50 employees) or industry (e.g., trades like plumbing, sole-trader service bookings, in-person retail). The exemption must apply to the entire business; partial eligibility only adds unnecessary complexity.

Recommendations:
We recommend rephrasing the wording of the exemption with a special focus on avoiding any requirements for a case-by-case analysis and introducing clear and objective criteria for the applicability covering a business as a whole and not only parts of it.

3.5. Data Breaches

Please see our feedback in the section on incident reporting.

4. Incident Reporting

The Commission is proposing an amendment to incident reporting obligations to streamline the reporting across different regulations. The amendments include:

- A single-entry point ("**SEP**") through which entities can simultaneously fulfil their incident reporting obligations under multiple legal acts. The SEP will be operated by ENISA who is distributing incoming reports to the relevant authorities. The subsequent process is then with the competent authority.
- The implementation of a common notification template covering the reporting requirements across the different regulations in one single form.
- In the GDPR, the threshold for notifying breaches is increased from "risk" to "high-risk". All breaches below the threshold need to be documented. The proposal also introduces criteria for assessing whether a breach qualifies as high-risk.
- For the GDPR, the deadline to notify a breach is extended from 72 to 96 hours.

Streamlining the intake of incident reports is not only welcomed by all stakeholders we consulted but is, from our experience, essential to ensure the proper functioning of the reporting obligation. Building on the proposed amendments we suggest considering some additional ones:

Under the GDPR, non-EU companies do not have a lead supervisory authority and are according to the Guideline by the EDPB on data breach notification[4] required to separately notify each data protection authority in every Member State where affected individuals are located. Given that there are 27 EU Member States, and Germany alone has 16 separate data protection authorities (one for each federal state), this can quickly become an overwhelming task. The amendments to the reporting obligations should explicitly clarify that the SEP is also available for reports by non-EU companies even if the subsequent steps are taken by the competent Member State authorities. This also means that the template to be developed needs to take into account reports by non-EU companies with questions on the location of affected data subjects. Single-entry Point must also mean single language to report.

Besides the intake, also the subsequent communication between authorities and the representative or the company would benefit from simplification especially in case of non-EU companies. A lot of the complexity of data breach notifications and the subsequent proceedings come from the very unique communication channels data protection authorities require companies to use, simple emails, PEC-emails or custom-made portals. If an authority requires communication through a portal, the requirements again are not harmonised, but every authority has its own isolated solution and often these isolated solutions have broken workflows or a flawed design. Some portals for example even block representatives or companies from other countries, even other Member States, from communication. This results in the impossibility of communication between the authority and the representative or the company. The easiest solution would be to change the EDPB Guideline on Data Breaches by award non-EU companies who appointed a representative with a single competent authority for a proceeding, namely the one where the representative is located. The concept of the single competent authority for non-EU companies is already well established in NIS 2, the DSA, or the Data Act. If such change of the EDPB Guideline on Data Breaches ins not supported, a streamlining of the authorities' communication channels would be required for an efficient and effective communication.

Furthermore, extending the deadline only for GDPR results again in different reporting requirements depending on the applicable regulations. Unifying the reporting deadlines would simplify the reporting overall and not only for the data breach reporting under the GDPR. Such unification could be accompanied by a preliminary report in specific cyber-risk cases.

[4] Guidelines 9/2022 on personal data breach notification under GDPR, Version 2.0, available under https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202209_personal_data_breach_notification_v2.0_en.pdf ("**EDPB Guideline on Data Breaches**")

Recommendations:
In addition to the proposed amendments we recommend considering additional amendments to:

- clarify that the SEP is also available to non-EU companies and taking the specifics of reporting by non-EU companies into consideration when developing the notification templates;
- adopting the concept of the single competent authority for non-EU companies as established under NIS 2, the DSA and the Data Act also for subsequent data breach proceedings after the initial notification which can be achieved by amending the EDPB Guideline on Data Breaches. If such amendment is not supported we want to highlight the need for streamlining the communication channels provided by authorities in incident and other proceedings;
- unify the reporting deadlines across the regulations in scope of the SEP.