ministry of digital affairs

14 October 2025

The Danish Government's response to the Commission's call for evidence for the Digital Omnibus as regards the digital area

A year after Mario Draghi's recommendations on *The future of European competitiveness* it is imperative to take decisive action to strengthen Europe's digital competitiveness, and Denmark encourages the Commission to present a Digital Omnibus that serves this end. It is of paramount importance that opportunities for simplification are considered without prejudice and with a high level of ambition. Therefore, we need to be open-minded and bold in pursuing genuine simplification throughout EU's digital framework.

Denmark fully supports the Commission's initiative to simplify the digital acquis and shares its ambition to reduce administrative burdens, simplify regulation and reduce fragmentation of the application of EU-law with a view to enhance competitiveness and innovation. We embrace a comprehensive review of the digital acquis, ensuring that all legislation is thoroughly assessed, and decisions are made on what should be retained, revised, or repealed. We furthermore welcome the digital fitness check to be introduced as an ongoing effort and hope that these processes will enable a more cohesive approach to the digital acquis focusing on improving alignment and suitability of the digital regulation.

Furthermore, we support the overarching objective behind the Digital Omnibus, focusing on targeted measures with immediate adjustments within areas where the same objectives can be achieved by less burdensome means. Consistent application and effective enforcement will be key. In this context, Denmark reiterates our strong commitment to support the Commission in its efforts towards reducing administrative burdens by 25 pct. overall and by 35 pct. for SMEs. In this endeavour, Denmark encourages the Commission to conduct impact assessments to get a better overview of the regulatory burdens before any new regulation is introduced – as well as changed.

To support the Digital Omnibus in achieving the objective of simplifying the digital acquis, the following section presents a summary of the Danish government's key suggestions. A detailed set of recommendations is outlined below and presented in greater detail in subsequent pages. It should be noted that this response does not include recommendations on cybersecurity, as this will be addressed in a separate contribution.

Specific recommendations (further detailed on page 4-16)

Data

The European data legislation should be simplified, streamlined and aligned in order for the horizontal legislation to provide a clear and consistent legal framework for data sharing and re-use with significantly fewer burdens for businesses. In particular, we encourage the Commission to:

1.1 Revise and simplify the data protection regime to reduce burdens for businesses and make it more innovation friendly, including by considering a more risk-based approach to data protection (GDPR).

1.2 Merge overlapping data legislation (including Free Flow of Non-Personal Data Regulation, Open Data Directive and Chapter II of Data Governance Act).

1.3 Ensure less stringent requirements for data intermediation in the Data Governance Act, for example by making the registration as a data intermediation service provider voluntary.

1.4 Provide guidance on correlated or overlapping legislative instruments, such as Data Act and GDPR regarding for example the distinction between personal and non-personal data.

1.5 Provide guidance on Data Act regarding complex data holder relationships and the relevance of product rules.

1.6 Ensure a demand-driven approach to requirements on public sector data sharing to create maximum effect.

1.7 Strengthen the mandate of the European Data Innovation Board (EDIB) and clarify the governance structure around the data acquis

1.8 Address legal uncertainties regarding use of public sector data, for example in the training of AI models

1.9 Encouraging data-driven solutions to simplify sharing of business data

Cookies and ePrivacy

Rules on cookies and online tracking technologies in the ePrivacy Directive should be updated and aligned with GDPR with a view to reduce burdens for European companies, while upholding the protection of data privacy. In this vein, we suggest the Commission to:

2.1 Abolish the cookie-banner for technical purposes and simple statistics (as now covered by article 13-15 in the GDPR).

2.2 Establish a structured dialogue for responsible authorities on cookies and tracking technologies to align enforcement and address cases of cross-border relevance.

2.3 Increase the liability for Consent Management Platforms (CMP) to address dark patterns and insufficient technical safeguards, thereby improving compliance.

2.4 Modernise the language and definitions of the ePrivacy directive to meet technological and legal developments.

2.5 Refrain from consolidating the ePrivacy Directive with the Data Act due to limited potential.

AI Act

The EU has demonstrated a firm commitment to take the lead in developing trustwothy AI. However, the rules have shown increasingly complex over time. In order to simplify the AI Act, while preserving the key objectives behind, we encourage the Commission to:

3.1 Extend the timelines for high-risk obligations by at least a year

3.2 Ensure proportional requirements for SMEs and start-ups

3.3 Safeguard coherence and avoid duplication with other digital EU legislation

3.4 Keep in mind that implementing acts on AI Regulatory Sandboxes could enable adaptable and flexible implementation

3.5 Remove the AI Literacy obligation and make it a non-binding guidance

3.6 Provide guidance on the term “vulnerable groups”

3.7 Balance proportionality and oversight by amending Article 49 on Registration Requirements

Electronic identification

Existing gaps, unclarities and obligations with limited added-value related to electronic identification should be addressed, ensuring that redundant burdens are removed. To this end, we encourage the Commission to:

eIDAS2

4.1 Remove references to legal persons from eIDAS2, by addressing this aspect comprehensively in a separate chapter of the Business Wallet regulation instead.

4.2 Introduce a “wallet-by-default”-principle to guarantee that the wallet-infrastructure is used in all relevant use-cases where there is value-added and demand.

4.3 Remove obligations for MS-specific certification schemes.

4.4 Reconsider Article 45e on Verification of attributes against authentic sources.

4.5 Create a category of attestation issuers which are not Trust Service Providers

4.6 Adjust the Open Source licensing requirement for EUDI Wallets in order to ensure necessary flexibility in contracting and development

Single Digital Gateway

4.7 Streamline synergies between the SDG-regulation and other legislation on electronic identification, by assessing whether the SDG-framework, including the OOTS, becomes redundant with the EBW.

4.8 Amend the definition of local services and include the definition in Article 3.

4.9 Amend article 14 to further clarify different mechanisms for exchange.

Specific recommendations in detail

1. Data

Recalling the Danish position outlined in the call for evidence on the European Data Union Strategy, we welcome the Commission's commitment to address concerns related to the current rules within the European data aquis, in view of ensuring their continued relevance and effectiveness. In particular, we encourage the Commission to streamline and consolidate existing legislation with the aim of reducing compliance burdens for European businesses and public authorities, and to unleash the full potential of data. In the following, we outline specific initiatives to consider:

1.1 Revise and simplify the data protection regime to reduce burdens for businesses and make it more innovation friendly, including by considering a more risk-based approach to data protection (GDPR)

While the protection of personal data is a fundamental right, which in its core shall be respected, the GDPR in its current form is creating barriers to the development and use of data-driven solutions such as AI that benefit European companies, citizens and public authorities. Where better data use could support the development of solutions that benefit European companies and citizens, the current regime risks stalling technological and societal innovation and limit Europe's chances to compete in the AI race.

A recent study finds that compliance with GDPR (and associated national legislation) costs Danish companies close to EUR 2 billion every year. There is an urgent need to address the negative effects of GDPR, which constitute a drag on European competitiveness.

Many initiatives in the private and public sector are being paused or abandoned due to concerns over compliance, stemming from GDPR rules that can be complex, unclear, and challenging to navigate without specialised legal expertise. In this vein, it is imperative to address uneven implementation and enforcement of the GDPR across Member States, in the aim of alleviating administrative burdens, in particular for European businesses engaged in cross-border activities in the EU.

Danish companies point to burdensome documentation requirements and mapping of data-flows and the broad scope of the rights granted to the data subjects. In particular, small companies and non-profit organizations find the GDPR burdensome to comply with. The impact is also felt by citizens — who find it more cumbersome to participate in community and volunteer organisations. From a Danish perspective it is very important to safeguard the continued functioning and prosperity of the civil society and local associations.

Thus, Denmark advocates for an upcoming revision of the GDPR that ensures that public authorities, businesses and individuals can benefit from data-driven solutions. Rather than hindering innovation, the revised framework should unlock improved access to data for the training of AI models.

There is no doubt that we need data protection in the EU. Nonetheless, we need to do it smarter and more flexible. Specifically, Denmark encourages an even more risk-based approach, where regulatory requirements are proportionate to the actual risks involved in data processing. Denmark sees a need to recalibrate the balance between, on one hand, ensuring an adequate level of protection of personal data, and on the other, ensuring the right scope of action for companies, so they can continue to thrive.

1.2 Merge overlapping data legislation (including Free Flow of Non-Personal Data Regulation, Open Data Directive and Chapter II of Data Governance Act)

Denmark encourages streamlining and improving coherence across the data acquis. This should include a thorough and ambitious review of the continued need for provisions of the data acquis, ensuring that only what remains relevant and effective is retained or added. In this context, it is important to carefully consider relevant upcoming proposals to assess which data-related legislative instruments could be meaningfully merged or aligned to reduce overlaps and complexity. It is also important to assess which legislative instruments should remain distinct to preserve legal clarity and purpose. Ultimately, providing a more coherent data acquis is about reducing overlap where it exists and streamlining relevant definitions, making it easier for authorities to enforce and for businesses to navigate their obligations and rights.

To this end, we propose to consolidate and merge legislation that governs overlapping areas, such as the Free Flow of Non-personal Data (FFoD), the Open Data Directive (ODD) and Chapter II of the Data Governance Act (DGA) on public sector data. Currently, it is unclear whether obligations fall under one or the other, creating unnecessary confusion for both public and private sector actors, as well as for national authorities, who must consult multiple legal texts covering the same subject matter.

The FFoD's provisions on cloud switching has been overtaken by the Data Act and can therefore be repealed. The work already invested in switching standards such as SWIPO (Switching Cloud Providers and Porting Data) should however be considered in the development of standards under the Data Act. The FFoD's prohibition against national data-localisation requirements remains very valid and should be retained but could be integrated in the Data Governance Act or in another data relevant act. The continued relevance of the transparency obligation regarding such localisation requirements should be assessed.

It is questionable whether the Data Act would be the right framework for a merging of the ODD, DGA and FFoD. Adding the ODD, the DGA and the FFoD to the Data Act would not *in itself* lead to administrative burdens for businesses and authorities when no clear cohesion exists. Also, the Data Act is already fragmented, covering several distinct areas and actors — for example Chapter II introduces obligations on data sharing from connected products, while Chapter VI requires easier switching between data processing services. At worst, simply merging different legislation with no clear overlap can lead to a more complex enforcement considering the division of labour between multiple competent authorities, thus not necessarily resulting in more clarity for businesses.

1.3 Ensure less stringent requirements for data intermediation in the Data Governance Act, for example by making the registration as a data intermediation service provider voluntary

We see merit in making the requirements for data intermediation service providers (Art. 12 of the Data Governance Act) less stringent, as the current rules make it difficult for companies to create a viable business model. Making the registration as a data intermediation service provider voluntary could be considered in this regard.

1.4 Provide guidance on correlated or overlapping legislative instruments, such as Data Act and GDPR regarding for example the distinction between personal and non-personal data

To genuinely reduce burdens for businesses and competent authorities, Denmark encourages the Commission to develop clear guidance on areas such as the interpretation of regulations, including examples of use cases as well as on delineations between overlapping or correlating legislative instruments.

One area where guidance is particularly needed is the relationship between the Data Act and the GDPR. While the Data Act is intended to supplement the GDPR, the distinction between personal and non-personal data will often be difficult to draw for data holders under Chapter II, particularly when datasets contain both types. Moreover, the Data Act introduces technical requirements for data sharing that affect how GDPR obligations are fulfilled, further blurring the boundaries between the two frameworks. This distinction is also highly relevant for the Free Flow of Non-Personal Data Regulation.

1.5 Provide guidance on Data Act regarding complex data holder relationships and the relevance of product rules

The Data Act constitutes a new set of rules regulating a previously unregulated areas, forming a general need for more guidance on the interpretation and real-life use of the Data Act – both for businesses and Member States.

Guidance is needed regarding the more complex relationships under Chapter II, such as manufacturers who outsource the data holder role, cases with multiple users, or cases with second-hand sellers. Article 3(2) of the Data Act requires sellers, renters, and lessors to provide users with specific information. In practice, this information will often have to come from the manufacturer of the connected product - likely in the form of a website link or a QR code on the product packaging. Guidance is needed for physical sellers/renters/lessors in cases where the manufacturers does not provide the information on the packaging of the product.

Furthermore, it would be helpful to further clarify the relevance of product rules and the European Commission's *"Blue Guide on the implementation of EU product rules"* (2022) in interpreting the Data Act. In particular, greater clarity is needed on the extent to which Article 3 of the Data Act should be read in light of product rules and the *Blue Guide*. This applies both to the definition of who qualifies as a manufacturer (for example, whether an actor who purchases a product and then relabels it with their own brand should be regarded as a manufacturer under the Data Act), and to the interpretation of disclosure obligations (for example, whether "clear and comprehensible" should be understood to imply the same language requirements as those set out in product rules).

The European Commission's FAQ, under Question 8, states that the *Blue Guide "served as inspiration for the Data Act's rules on products and provides comprehensive guidance on this topic. For instance, the Blue Guide identifies situations where a product is not considered to be 'placed on the market'*." However, the extent to which the principles of the *Blue Guide* should apply in a Data Act context remains unclear.

1.6 Ensure a demand-driven approach to requirements on public sector data sharing to create maximum effect

We encourage allowing for a demand driven approach to spend the resources required for making data available where these efforts can create maximum effect rather than chasing mindless publication of more and more datasets with limited reuse value. Rather than a more stringent requirements on public sector data sharing such as mandatory APIs or expanding the scope of high value datasets.

1.7 Strengthen the mandate of the European Data Innovation Board (EDIB) and clarify the governance structure around the data acquis

There is a need to clarify and strengthening the governance structure around the digital acquis by improving the composition of the European Data Innovation Board (EDIB) and strengthening its mandate, and we suggest aligning it better with other fora such as the Open Data Committee and the IEB.

1.8 Address legal uncertainties regarding use of public sector data, for example in the training of AI models

Further, fragmentation in the EU's data legislation can create legal uncertainty, e.g. when public authorities seek to train AI models. To address this EU-level guidance could be provided on the lawful bases for re-use of public sector data, especially in the AI context, e.g. how the purpose limitation principle (Article 5(1)(b) GDPR) is to be interpreted. In the same vein, robust and harmonised EU standards for anonymisation and pseudonymisation could be considered, giving public authorities the necessary legal certainty when sharing or releasing data sets.

1.9 Encouraging data-driven solutions to simplify sharing of business data

As a more horizontal point, we wish to highlight the importance to advance and ensure common standardised data, structured data formats and enhance cross-border interoperability between digital business systems efficiently reducing the burdens stemming from non-standardised data, fragmented digital ecosystems and manual processes within companies.

2. Cookies and ePrivacy

There is an urgent need to modernise the EU regulatory framework on cookies and online tracking to reduce burdens for European businesses and address persistent issues, including consent fatigue and information overload, fragmented and uneven enforcement and technological developments in the market. It is therefore imperative to move forward, refining and updating key elements of the ePrivacy Directive to ensure a less burdensome framework for business in EU while upholding the protection of data privacy. To this end, a number of measures should be considered.

2.1 Abolish the cookie-banner for technical purposes and simple statistics (as now covered by article 13-15 in the GDPR).

We urge the Commission to consider the interaction between the GDPR and the ePrivacy Directive. The ePrivacy Directive requires end-users' informed consent before storing cookies or other online tracking technologies on a user's device. In other words, all providers of websites or apps find themselves in need of a cookie banner in order to fulfill the requirements for consent of the end-user.

The costs related to implementing and maintaining a cookie banner are substantial. The majority of all European companies own websites, which collect and process end-user's data for technically necessary functions and for conducting simple statistics for the functioning and use of their website. From a privacy perspective, these tracking purposes are to be considered harmless. Hence, there are huge costs reductions to be made for European companies, if collection and processing for these purposes are clearly exempted from prior consent. In effect, only companies collecting data for other purposes, *e.g.*, marketing or sharing of data with third parties, would be required to maintain cookie banners.

In practice, this scenario could most clearly be implemented by changing the GDPR as well as the ePrivacy Directive. The ePrivacy Directive defines the term consent through a reference to the GDPR. This link between the two regulations makes good sense, as GDPR can require consent from a legal person, the data subject, for the processing of personal data, even if the ePrivacy Directive did not require consent to collect and process the end-user's communications data. Thus, it could be appropriate to make an exemption in the GDPR, whitelisting the processing and storage of personal communications data for technical purposes and for simple statistics.

Amendments for Regulation (EU) 2016/679 (GDPR) to implement recommendation 2.1

It is recommended that a minimum threshold is implemented when it comes to **Article 13-15** of the GDPR. For instance, by introducing a lower limit for the processing activity required before the rights of the data subject apply. In particular, the right of access by the data subject under Article 15 of the Regulation is thus perceived by many controllers as a particularly burdensome right to comply with. It should also be considered to ease the requirements and / or to expand the exceptions to Article 13.

Further, it is suggested that the need for Article 20 of the GDPR is reconsidered, as the provision appears to be more in the nature of a consumer right.

2.2 Establish a structured dialogue for responsible authorities on cookies and tracking technologies to align enforcement and address cases of cross-border relevance

The ePrivacy Directive regulates many service providers operating across EU borders, which has created challenges for enforcement at the national level. Providers often face cases being opened simultaneously in different Member States, along with diverging interpretations of the rules depending on the jurisdiction. We recommend establishing an EU-level advisory board or coordinating forum that could issue expert opinions on cases of cross-border relevance, which are not well-suited to be handled solely at the national level. This could potentially be a done under the auspices of the EDPB or the EDIB. In the long-term further harmonisation of requirements and enforcement could be considered.

2.3 Increase the liability for Consent Management Platforms (CMP) to address dark patterns and insufficient technical safeguards, thereby improving compliance

Currently, website and app owners bear sole responsibility for complying with legal requirements, even though they often rely on CMPs to handle user consent. CMP providers, however, carry no direct legal responsibility. This imbalance has led to weak compliance, widespread use

of dark patterns in cookie banners, and insufficient technical safeguards to prevent tracking before consent is given.

To address this, a clear legal framework should be established to define the extent to which CMP providers can be held jointly responsible for compliance. Such a framework would strengthen cookie banner practices, reduce the reliance on manipulative design patterns, and improve technical safeguards to ensure that tracking does not occur without consent. Redistributing responsibility in this way would reduce the burden on website owners, while requiring CMP providers to assume greater accountability.

Concretely, CMPs should be required to provide default solutions that comply with existing legislation. If a website owner chooses to alter or disable these default compliance features, the CMP should be legally obliged to advise them of the potential legal risks. For example, if a website owner attempts to remove the option to "reject all tracking technologies," the CMP must explicitly inform them that such an action is likely unlawful.

This rebalancing of responsibility could be achieved through a legislative amendment, ensuring that CMP providers play an active role in upholding legal standards while supporting both businesses and consumers in the digital environment.

2.4 Modernise the language and definitions of the ePrivacy directive to meet technological and legal developments

When reviewing and applying the ePrivacy Directive, it becomes clear that the regulation relies on outdated terminology. We recommend updating its language and definitions to better reflect the evolving digital landscape and to ensure consistency with other relevant EU digital legislation. Furthermore, it should also be assessed if all rules are still needed given the technological developments, and it should be ensured that similar services are subject to the same rules. This would provide much-needed legal clarity and greatly benefit both consumers and businesses, who often find the current directive difficult to interpret.

2.5 Refrain from consolidating the ePrivacy Directive with the Data Act due to limited potential

While consolidating the ePrivacy Directive with the GDPR and the upcoming Digital Networks Act could create synergies by aligning similar and compatible rules on on the one hand data protection and oversight and on the other hand electronic communications providers, the Data Act does not regulate comparable issues. Incorporating the ePrivacy Directive into the Data Act would therefore risk complicating an already fragmented legal framework and would make supervision at the national level more difficult.

3. AI Act

The European Union has shown its strong commitment to lead in trustworthy artificial intelligence (AI), notably through the adoption of harmonised rules in the Artificial Intelligence Act (AI Act). The Act lays down a risk-based regulatory framework with concrete requirements for, e.g., high-risk AI systems. In the following we propose ideas for how to simplify the regulation without compromising the fundamental objectives of the Regulation.

3.1 Extend the timelines for high-risk obligations by at least a year

The current compliance deadlines for high-risk obligations set in AIA, chapter III, risk overwhelming providers, particularly SMEs and start-ups. Compliance depends heavily on the

timely availability of harmonised standards, both of which are still under development and will be at least one year delayed. The Commission guidelines is likewise significantly delayed. Imposing full obligations before this framework is in place creates legal uncertainty and disproportionate burdens on businesses and risk undermining the development and uptake of AI in Europe.

We therefore propose extending the implementation timelines for high-risk AI systems by at least one year, allowing providers and deployers to adapt once the standards are available as originally foreseen during negotiations. This can be achieved via targeted amendments to article 113 of the AI Act on "Entry into force and application". We believe this is a fair and balanced approach that makes compliance more realistic for providers and deployers, while maintaining constructive pressure on standardisation organisations to finalise harmonised standards as quickly as possible.

3.2 Ensure proportional requirements for SMEs and start-ups

SMEs should not be required to meet the same resource-intensive obligations as larger providers as their systems are unlikely be as widespread in use and therefore unlikely to pose the same level of risk. The volume of individual documentation, registration and assessment for providers of high-risk AI systems poses a significant burden. Fulfilment should be proportionate to the resources and capacity of the provider and to the risk posed by the systems. Some requirements are particularly challenging for SMEs and start-ups. We therefore suggest the following adjustments.

Firstly, we suggest an exception is made to article 11(1) on "Technical documentation", so that SMEs and start-ups only have to provide technical documentation upon request. Currently, article 11 obliges providers to prepare and maintain full technical documentation before placing an AI system on the market, which requires substantial ongoing administrative effort. Currently, article 11(1) states that "SMEs, including start-ups, may provide the elements of the technical documentation specified in Annex IV in a simplified manner". We suggest to clarify the article to make it clear that providers are only required to provide technical documentation upon request. This would be a more proportionate approach, ensuring accountability, while avoiding unnecessary costs.

Secondly, we suggest extending the derogation in article 63(1) on "Derogations for specific operators" to SMEs and start-ups, as quality management systems and post-market monitoring are among the most expensive compliance elements; a narrowly scoped exemption would alleviate some of the burdens while preserving safety objectives.

3.3 Safeguard coherence and avoid duplication with other EU legislation

To support a well-functioning single market for AI development and deployment, the AI Act must be implemented consistently, predictably and coherently with other frameworks notably the GDPR. For example, article 27 in the AI Act introduces an obligation that is overlapping with article 35 in GDPR in scope. Article 27 requires deployers to self-assess potential impacts of high-risk AI systems on fundamental rights before placing a system on the market. This places a heavy burden on companies, especially SMEs, which often lack the expertise for such complex assessments.

We therefore propose removing the article 27 self-assessment for companies and relying instead on the post-market supervisory role of Article 77 bodies, namely national public authorities or bodies protecting fundamental rights. Under the suggested approach, Article 77 bodies would monitor whether companies uphold their fundamental rights obligations, similar to the way market surveillance authorities s supervise other AI Act obligations. This would be more efficient and reliable.

In line with the risk-based approach and to avoid double notifications, we would also recommend reconsidering the classification of 'any' infringement of EU law obligations intended to protect fundamental rights as a "serious incident" in article 3(49)(c). Such infringements are already subject to appropriate sanctions under the relevant laws. Additional AI Act notifications are unlikely to significantly improve protection and will generate large volumes of reports, which will draw resources from genuinely serious incidents, covered under the other points in article 3(49). We therefore recommend deleting point c.

Furthermore, the AI Act introduces extensive obligations, particularly for high-risk systems used in the public sector. Uncertainty on risk classification and compliance risks regulatory paralysis or inadvertent non-compliance. To mitigate this, the Commission should develop clear and user-friendly guidance on integrated impact assessments, bringing together AI Act articles 9 and 27 (risk management & fundamental rights), GDPR article 35 (Data Protection Impact Assessment), and NIS2 article 21 (cybersecurity risk management). A single, coherent methodology would enable straightforward, timely and correct compliance.

3.4 Keep in mind that implementing acts on AI Regulatory Sandboxes could enable adaptable and flexible implementation

The AI regulatory sandboxes can be highly beneficial if they remain flexible and do not overburden Member States and participants with detailed procedural requirements. Implementing acts should allow for adaptable setups and avoid disproportionate administrative obligations for hosting authorities.

3.5 Remove the AI Literacy obligation and make it a non-binding guidance

We suggest removing article 4 and making it a non-binding recommendation. At present, the requirement is widely misunderstood and often over-implemented due to fear of non-compliance. It is particularly unclear what constitute "sufficient AI-literacy", and unproportionate amounts of resources are spent on uncovering it.

3.6 Provide guidance on the term "vulnerable groups"

Article 9(9) requires providers to consider the likelihood of negative impacts on minors and, where relevant, other vulnerable groups when implementing article 9 (1-7). The objective is important, but further guidance is needed to keep *requirements* practicable. Any guidance on "vulnerable groups" under article 9(9), should take into account existing guidance and interpretations related to the prohibited AI practices.

3.7 Balance proportionality and oversight by amending Article 49 on Registration Requirements

The AI Act requires certain providers of high-risk AI systems to register products in a central EU database prior to market placement. While transparency is a legitimate aim, the mechanism as designed risks imposing disproportionate burdens, especially on SMEs and start-ups, without clear benefits for end-users or regulators.

A more proportionate approach would be to either remove the requirement in article 49 entirely or amend it so that registration obligations are streamlined and limited to essential, non-sensitive information. Ideally, the necessary information would be shared through a Digital Product Passport rather than a new database.

4. Electronic identification

With regard to simplification towards aspects related to electronic identification under the European Digital Identity Framework, including the forthcoming proposal on a European Business Wallet, Denmark reiterates the position laid out in Denmark's response to the Call for Evidence on the European Business Wallet (EBW). In addition, the following section presents key recommendations for simplifying Regulation (EU) 2024/1183 (eIDAS2).

Recommendations on eIDAS2

4.1 Remove references to legal persons from eIDAS2, by addressing this aspect comprehensively in a separate chapter of the Business Wallet regulation instead.

When introducing the EBW it is suggested that the existing infrastructure gaps are addressed first. To this end, we recommend removing references to legal persons from eIDAS2, addressing this aspect comprehensively in a separate chapter of the Business Wallet regulation instead. In this context, Denmark supports the principle behind the "one in, one out" approach in relation to the publication of the EBW initiative, as we understand it to reflect a commitment to reduce unnecessary burdens on businesses, ensuring that new obligations introduced through the EBW are offset by the removal of redundant requirements and burdens under eIDAS and eIDAS2.

4.2 Introduce a "wallet-by-default"-principle to guarantee that the wallet-infrastructure is used in all relevant use-cases where there is value-added and demand.

We echo the need for a "wallet-by-default"-principle to ensure that the wallet-infrastructure is used in all relevant use-cases where there is value-added and demand. This would, among other things, ensure that both the EUDI Wallet and European Business Wallets would be widely used for authentication purposes in EU legislation.

4.3 Remove obligations for MS-specific certifications schemes in eIDAS2

While transparency and trust in the Wallet require that user-facing components remain open source, a blanket obligation to open-source all application software components risks reducing flexibility in procurement, contracting, and development. Many Member States rely on private contractors who use proprietary modules, libraries, or integration layers that cannot legally or commercially be licensed under open-source terms.

The strict obligation to open source license all components installed on the user device may discourage private-sector participation, limit innovation, and increase costs by forcing custom-made development rather than reuse of existing solutions. A strict requirement that all wallet components on the user's device must be open-sourced may hinder Member States' ability to contract flexibly with private developers, especially where proprietary modules or licensed elements are embedded. For some implementations, it may be legally or commercially impossible to release such components under an open-source license without undermining security or intellectual property rights.

Member States should retain the option to exempt specific components — including those on user devices — where duly justified. Safeguards can be maintained through e.g. closed disclosure to authorities or civil society organisations. This maintains transparency for users, while giving Member States necessary flexibility to procure and develop Wallet solutions efficiently.

Suggestions for Regulation (EU) 2024/1183 (eIDAS2) to implement recommendation 4.3

DRAFTING SUGGESTION FOR ARTICLE 5c:

"3. For requirements referred to in paragraph 1 of this Article that are not relevant for cybersecurity, and, for requirements referred to in paragraph 1 of this Article that are relevant for cybersecurity, to the extent that cybersecurity certification schemes as referred to in paragraph 2 of this Article do not, or only partially, cover those cybersecurity requirements, also for those requirements, **the Commission must establish one or more complete certification schemes for the commonly recognized architectural profiles for use by conformity assessment bodies across the Union, taking into account the need for different wallet implementations across Member States.** Member States ~~**shall**~~ **may also** establish national certification schemes following the requirements set out in the implementing acts referred to in paragraph 6 of this Article. Member States shall transmit their draft national certification schemes to the European Digital Identity Cooperation Group established pursuant to Article 46e (1) (the 'Cooperation Group'). The Cooperation Group may issue opinions and recommendations."

4.4 Reconsider Article 45e on Verification of attributes against authentic sources in eIDAS2

Article 45e, as drafted, obliges all Member States to open authentic sources for verification by Qualified Trust Service Providers (QTSPs). This wide obligation risks a costly and far-reaching implementation, while potentially also undermining the subsidiarity principle and the flexibility Member States need in organizing their identity infrastructures.

We find the objective of Article 45e regarding the verification by QTSPs to be unclear. If the intention is for QTSPs to issue Public-sector attributes listed in Annex VI (e.g., civil status, nationality, residence) as Qualified Electronic Attestation of Attributes (QEAAs), this may not be relevant in some Member States, as they may wish to retain exclusive control over issuance, ensuring these attributes are only released as Public-Sector Electronic Attestation of Attributes (Pub-EAAs) directly from the competent authority. Others may see value in enabling QTSPs to verify and issue attributes on request. Both models are valid and should remain at the discretion of the Member State.

For smaller administrations in particular, creating and maintaining secure interfaces for external QTSP verification is costly and administratively burdensome. Moreover, delegating access to authentic sources raises governance and liability issues that some Member States may prefer to avoid.

Therefore, Article 45e should be reframed to say that Member States may enable QTSPs to verify attributes against authentic sources, but are not obliged to do so. See appendix X for Article specific suggestions.

Suggestions for Regulation (EU) 2024/1183 (eIDAS2) to implement recommendation 4.4

DRAFTING SUGGESTION FOR ARTICLE 45e:

"1. Member States ~~**shall ensure, within 24 months of the date of entry into force of the implementing acts referred to in Articles 5a(23) and 5c (6), that, at least for the attributes listed in Annex VI, wherever those attributes rely on authentic sources within the public sector,**~~ **may take** measures ~~**are taken**~~ to allow qualified trust service providers of electronic attestations of attributes to verify **attributes that rely on authentic sources within the public sector** ~~**those attributes**~~ by electronic means at the request of the user, in accordance with Union or national law."

4.5 Create a category of attestation issuers which are not Trust Service Providers in eIDAS2

Today, issuing EAAs is a trust service by design. eIDAS2 makes "issuance of Electronic Attestation of Attributes" a new trust service; providers of qualified and non-qualified EAA services are regulated as TSPs. That means any private issuer that wants to place EAAs into wallets steps into the eIDAS trust-service regime. Even non-qualified TSPs face formal obligations (risk management, 24-hour incident/breach notifications to the supervisor, etc.), and eIDAS2 sets administrative-fine ceilings that can reach €5M or 1% of worldwide turnover — deterring SMEs and sector issuers whose attributes are low-risk (e.g., training completions, memberships, loyalty status).

Wallet adoption needs many 'everyday' attestations. eIDAS2 already reserves stricter tracks for (i) public-sector authentic-source attestations and (ii) qualified EAAs. But there is no lightweight, clear pathway for private issuers of routine attributes to participate without becoming TSPs. The gap slows ecosystem growth and creates uncertainty for companies "outside the realm of eIDAS" about what they commit to.

Legal certainty can be preserved without full TSP status. eIDAS2 already grants baseline legal effect to EAAs (they can't be dismissed just for being electronic or non-qualified). Preserving that baseline while creating a lighter issuer category would keep relying parties free to weigh probative value case-by-case, while avoiding disproportionate supervisory burdens for low-risk use cases

4.6 Adjust the Open Source licensing requirement for EUDI Wallets in order to ensure necessary flexibility in contracting and development in eIDAS2

While transparency and trust in the Wallet require that user-facing components remain open source, a blanket obligation to open-source all application software components risks reducing flexibility in procurement, contracting, and development. Many Member States rely on private contractors who use proprietary modules, libraries, or integration layers that cannot legally or commercially be licensed under open-source terms.

The strict obligation to open source license all components installed on the user device may discourage private-sector participation, limit innovation, and increase costs by forcing custom-made development rather than reuse of existing solutions. A strict requirement that all wallet components on the user's device must be open-sourced may hinder Member States' ability to contract flexibly with private developers, especially where proprietary modules or licensed elements are embedded. For some implementations, it may be legally

or commercially impossible to release such components under an open-source license without undermining security or intellectual property rights.

Member States should retain the option to exempt specific components — including those on user devices — where duly justified. Safeguards can be maintained through e.g. closed disclosure to authorities or civil society organisations. This maintains transparency for users, while giving Member States necessary flexibility to procure and develop Wallet solutions efficiently.

Suggestions for Regulation (EU) 2024/1183 (eIDAS2) to implement recommendation 4.6

DRAFTING SUGGESTION FOR ARTICLE 5a:

"3. The source code of the application software components of European Digital Identity Wallets shall be open-source licensed. Member States may provide that, for duly justified reasons, the source code of specific components ~~**other than those installed on user devices**~~ shall not be disclosed. **Member States shall ensure that, in such cases, appropriate measures are in place to guarantee transparency, security, and interoperability**"

Recommendations on the SDG (Single Digital Gateway Regulation)

4.7 Streamline synergies between the SDG-regulation and other legislation on electronic identification, by assessing whether the SDG-framework, including the OOTS, becomes redundant with the EBW.

In addition, with the introduction of the EBW we recommend that the potential double implementation when it comes to the Once-Only Technical System (OOTS), as laid out in the SDG EU 2018/1724, is considered and assessed further. We therefore urge the Commission to examine whether use cases and interactions currently covered by the OOTS could be more effectively supported through the EWB framework, and whether such cases should consequently be exempted from exchange via the OOTS.

In this vein, it is suggested that the synergies between the SDG and other legislation related to electronic identification is streamlined in order to reduce administrative burdens. Therefore, two further amendments on the SDG are proposed below.

4.8 Amend the definition of local services and include the definition in Article 3

Currently, the exception of certain national procedures from being made fully accessible online due to being highly localised is briefly described in SDG preamble 20. However, this brief and surface-level description has led to confusion over what is to be considered as a local service and its practical implications, as our mapping of the Danish procedure portals has uncovered a wide range of procedures that in theory fall within the purview of Annex II but have few to no cross-border users annually, or where all the documentation, that is requested during the procedure, is issued by another Danish Competent Authority. We therefore propose that the description of such exceptions in preamble 20 is amended, and that its definition is included in Article 3 regarding definitions.

Suggestions for Regulation (EU) 2018/1724 (SDG) to implement recommendation 4.8

Preamble 20: "For cross-border users who are not resident or established in the Member State concerned, online national procedures that are not relevant for the exercise of their internal market rights **(local procedures)**, for instance enrolment in order to receive local services, ~~such as garbage collection and parking permits,~~ do not need to be made fully accessible online. **Where such procedures are already accessible online, they do not need to be connected to the OOTS.**"

Article 3, (new) paragraph 6: "Local procedures are defined as procedures that require the user to have a pre-established connection to the Member State concerned, i.e. registering for residential garbage collection or applying for residential parking permits; national procedures that have few to no cross-border users annually; and national procedures that exclusively require information and/or documentation issued by the Member State of the said national procedure."

4.9 Amend article 14 to further clarify different mechanism for exchange

Article 14, paragraph 10 in the SDG already contains an exception of document exchange where different mechanisms for the exchange of evidence are already established at Union level. However, since the drafting of the SDG, the inception of eIDAS2 regulations made it clear that there is a not insignificant volume of evidence that is to be exchanged both via the OOTS and the EUDI Wallet. Additionally, there also exists an overlap between information that is relevant to the procedures in Annex II and information that is already made publicly available by issuing Competent Authorities in accordance with existing EU-regulation.

Consequently, the exchange of information via the OOTS that is either already publicly available or will also be exchanged via the EUDI Wallet is in practice a costly double implementation that contains no additional benefit to neither the requesting nor the providing Competent Authorities – or even to the end-user carrying out the online procedure. To avoid such an unnecessary and burdensome dual implementation, we propose that Article 14, is amended to include the EUDI Wallet and publicly available information as different mechanisms for exchange, by inserting these as paragraphs 11 and 12, respectively, with the existing paragraph 11 becoming paragraph 13.

Suggestions for Regulation (EU) 2018/1724 (SDG) to implement recommendation 4.9

Article 14

"(new) 11. Paragraphs 1 to 8 shall not apply to procedures and documentation that are covered by the EUDI Wallet as set out in EU 2024/1183."

"(new) 12. Where the requested information is already made publicly available by the issuing Competent Authority and thereby already accessible to the requesting Competent Authority, this shall be considered as a different mechanism for evidence exchange in accordance with those described in paragraph 10, and paragraphs 1 to 8 shall therefore not apply to such publicly available information."