Brussels, October 2025

BSP Position Paper: Digital Omnibus

Business & Science Poland

This position paper is submitted on behalf of Business & Science Poland (BSP) *in response to the European Commission's Call for Evidence on the "Digital Omnibus" (Digital Package on Simplification). It addresses the Commission's identified areas of concern with concrete simplification proposals drawn from industry experience.*

Background

The European Union's digital regulatory landscape has grown complex, with overlapping obligations that disproportionately burden European innovators. Such heavy burdens can be handled mainly by the largest enterprises - often from outside the EU - whereas young innovative companies give up on operations in the European market. The EU's regulatory approach often slows innovation, as varying national requirements, overlapping supervisory bodies and excessive implementation ("gold-plating") discourage digital firms from operating across borders. Moreover, restrictions on data storage and processing raise operational costs and limit the creation of large datasets vital for AI development, while differing public procurement rules across Member States further increase the fixed costs faced by cloud service providers.

This reality underscores the urgent need to **reduce unnecessary bureaucratic barriers and simplify the entire ecosystem of EU digital regulations**, so as to **unlock innovation potential in the EU's Single Market**. BSP therefore welcomes the Commission's initiative to streamline the *data acquis*, ePrivacy rules on cookies, cybersecurity incident reporting, & AI Act implementation.

Key BSP recommendations

Data *Acquis* - Data Act

- Limit the range of devices covered by the Data Act so as to exclude key consumer devices such as personal computers, tablets, smartphones, and smartwatches.
- Narrow the scope of data covered in order to avoid duplication with the GDPR and conflicts with the Digital Markets Act.
- Restrict the obligation to share data between businesses and the public sector (currently applying to unspecified "data") solely to product data and service-related data.

Rue Belliard 40, 1000 Brussels
e-mail: info@zpbsp.com
EU Transparency Register Number: 548212735276-89

ePrivacy Directive - cookies and other tracking technologies

- Extension of the exemption from the consent requirement under Article 5(3) of the ePrivacy Directive to cover cookies and other forms of access to, or storage of, data on a device for security-related purposes.
- Extension of the exemption from the consent requirement under Article 5(3) of the ePrivacy Directive to cover cookies and other forms of access to, or storage of, data on a device for analytical purposes.
- Extension of the exemption from the consent requirement under Article 5(3) of the ePrivacy Directive to cover cookies and other forms of access to, or storage of, data on a device for the purpose of displaying contextual advertising to users.
- Clarification that displaying a cookie banner is not required where one of the exemptions under Article 5(3) applies (i.e. when user consent is not necessary).
- Clarification that "storing information or gaining access to information already stored" does not cover short-term storage or information transmitted as part of a normal internet connection.
- Partial repeal of provisions on direct marketing.
- Partial repeal and harmonisation of provisions on traffic data.

Cybersecurity related incident reporting obligations

- A single EU-wide reporting mechanism: designate and equip one Union-level authority responsible for receiving incident notifications, establishing a unified portal and a single reporting form applicable under the above-mentioned regulations.
- Harmonisation of reporting elements:
  Thresholds: standardise the definitions and reporting thresholds for incidents across different regulations (e.g. aligning the concepts of "severe" and "significant").
  Deadlines: review and harmonise incident reporting deadlines, adopting a 72-hour deadline as a general standard to ensure consistency and reduce the burden on incident response teams.
  "Report once, comply with many" principle: a report submitted under one key regulation (e.g. the NIS2 Directive) should be deemed to fulfil the reporting obligations under other relevant legal acts (e.g. the Directive on the Resilience of Critical Entities).

AI Act implementation

- Adoption of a proportionate, risk-based approach to fine-tuning, through guidelines of the AI Office and implementing acts, recognising that existing rules already cover most risks, clarifying that original providers are not liable for third-party changes, classifying modifications by technical nature not by actor, allowing reassessment based on actual capabilities, simplifying update obligations, and applying full requirements only to significant fine-tuning.
- Limitation of the territorial scope of obligations related to copyright law, particularly through exemptions for text and data mining, restricting Article 53 to activities under EU law, clarifying its alignment (not extension) with existing copyright provisions, and preventing interpretations that could cover website indexing or conflict with search engine functions.
- Verification of computational thresholds for general-purpose AI models and systemic risk, raising thresholds to realistic levels (10^{23} and 10^{26}), setting modification limits relative to the base model's computational power, and introducing a roadmap for adaptive future adjustments.
- Simplification of self-assessment for high-risk AI, requiring clear Commission guidelines by February 2026, recognising good-faith self-assessments as valid unless proven otherwise, and allowing simplified documentation where no substantial risk exists.
- Revision of the regulatory approach to general-purpose AI, restoring the original technologically neutral concept of the Act and removing Chapter V and related recitals.
- Adoption of an efficient mechanism for resolving cross-border disputes, introducing in Chapter VII a model based on the "one-stop-shop" or "country of origin" principle.

Detailed Recommendations

I. Data *Acquis*

Data Act: Refine scope and reduce overlap with existing regimes - Key amendments should narrow the definition of "connected product" in Article 2(5) to exclude consumer devices such as PCs, tablets, smartphones, and smartwatches, whose main purpose is not data transmission. Chapter II should cover only B2B-generated data, excluding consumer-generated information already governed by the GDPR and the Digital Markets Act, and remove obligations for unreadable or non-useful datasets. The absolute ban on data sharing with "gatekeepers" should be replaced by a prohibition on coercive practices only. Chapter V (B2G) should be limited to product and related-service data,

with transparent lists of public bodies authorised to request access. These technical refinements would reduce compliance burdens, prevent legal duplication, and align the Act with existing EU data and digital frameworks.

Detailed Recommendations – Data Act

Simplification #1**: Narrowing the Scope of the Term "Connected Product"**	
Proposed change	**Justification**
Exclusion of certain types of hardware products from the scope of the Data Act, through an amendment to Article 2(5): "*5. 'connected product' means an item that obtains, generates or collects data concerning its use or environment and that is able to communicate product data via an electronic communications service, physical connection or on-device access, and whose primary function is not the storing, processing or transmission of data on behalf of any party other than the user; however, this does not include products that have been designed primarily for the purpose of displaying or playing content, or for recording and transmitting content, including for the use of an online service."* Such products include, among others, personal computers, tablets, smartphones and smartwatches.	The proposed amendment aims to exclude a range of products from the scope of the **Data Act** in order to reduce the compliance burdens associated with these categories of products. The Commission's original proposal for the Data Act included such an exclusion, which serves as the basis for this proposed change. The objective of the Data Act is to strengthen the EU's data-driven economy and support a competitive data market by increasing the availability and usability of data (in particular industrial data), fostering data-based innovation, and improving data accessibility. In practice, however, the broad scope of obligations arising under the Data Act hinders innovation by imposing significant burdens on entities that must comply with ambiguous provisions which, in some cases, conflict with other EU legal regimes (see also Simplification #2 below). This amendment is therefore intended to reduce those burdens by **narrowing the scope of application** of the Data Act
Alternative Proposal to the Previous Recommendation - Exclusion of Smartphones from the Scope of the Data Act: "*5. 'connected product' means an item that obtains, generates or collects data concerning its use or environment and that is able to communicate product data via an electronic communications service, physical connection or on-device access, and whose primary function is not the storing, processing or transmission of data on behalf of any party other than the user; however, this does not include smartphones."* New definition of "smartphone" under Article 2 of the Data Act:	The proposal aims to narrow the definition of a **"connected product"** by excluding **smartphones** from its scope. Smartphones represent a category of connected product that could significantly broaden the application of the **Data Act**, as a wide range of applications could be classified as **"related services"** associated with smartphones. As a result, this simple amendment could substantially reduce the compliance burden on entities by clarifying that the types of **connected products** and **related services** for which compliance solutions must be developed under the Data Act do not include smartphones or their related services (i.e. applications).

"smartphone" means a mobile telephone (within the meaning of Article 2(1) of Regulation (EU) 2023/1670) that has the following characteristics: *(a) it features wireless network connectivity, mobile access to internet-based services, an operating system optimised for handheld use, and the capability to accept both proprietary and third-party software; and* *(b) it is equipped with an integrated display incorporating a touchscreen.*	
Simplification #2: **Exclusion from the Scope of Chapter II of Data Generated through the Use of Connected Products or Related Services by Consumers**	
A targeted amendment to Article 7 of the Data Act, narrowing the scope of Chapter II by excluding consumer data: *"CHAPTER II* *~~BUSINESS TO CONSUMER AND~~ BUSINESS TO BUSINESS DATA SHARING* *[...]* *Art. 7 Scope of ~~business-to-consumer~~ and business-to-business data sharing obligations* *1. The obligations of this Chapter shall not apply to:* *a) data generated through the use of connected products manufactured or designed or related services provided by a microenterprise or a small enterprise, provided that that enterprise does not have a partner enterprise or a linked enterprise within the meaning of Article 3 of the Annex to Recommendation 2003/361/EC that does not qualify as a microenterprise or a small enterprise and where the microenterprise and small enterprise is not subcontracted to manufacture or design a connected product or to provide a related service.* *a) data generated through the use by consumers of connected products or related services provided to consumers;* *b) data generated through the use of connected products manufactured or designed, or related services provided, by a microenterprise or a small enterprise, provided that such an enterprise has no partner enterprise or linked enterprise within the meaning of Article 3 of the Annex to Recommendation 2003/361/EC which does not*	As a result of this change, only data generated in a **B2B context** through the use of connected products and related services would fall under the obligations concerning **data portability and information provision** set out in Chapter II. In addition, the **pre-contractual information obligations** would apply solely to B2B relationships. **Risks of inaction** The justification for this change lies in the fact that the **GDPR** and the **Digital Markets Act (DMA)** already adequately ensure the right to data portability in relation to consumer use of connected products and related services; therefore, imposing additional and overlapping obligations under the Data Act would be redundant and excessively burdensome. The same reasoning applies to **pre-contractual information obligations** under Article 3(2) and (3), which overlap with the GDPR and could overburden consumers with additional (albeit very similar) information. The average user would be unlikely to distinguish between information provided under the GDPR and that required by the Data Act. **Benefits of adopting this recommendations** Finally, excluding data generated by consumer products, which in many cases constitute **personal data**, from the data portability obligations under Chapter II aims to reduce the **risk borne by data holders** in connection with potential breaches of the GDPR.

qualify as a microenterprise or small enterprise, and that the microenterprise or small enterprise is not a subcontractor commissioned to manufacture or design the connected product or to provide the related service. *c) ~~The same shall apply~~ to data generated through the use of connected products manufactured by or related services provided by an enterprise that has qualified as a medium-sized enterprise under Article 2 of the Annex to Recommendation 2003/361/EC for less than one year and to connected products for one year after the date on which they were placed on the market by a medium-sized enterprise.*	
Alternative Proposal to the Previous Recommendation – Targeted Amendment to Article 7 to Exclude Data That Are Not Useful to the Recipient or User: "*1. The obligations of this Chapter shall not apply to:* *a) data generated through the use of connected products or related services that are held by the data holder in an **unreadable form**, such that their disclosure would provide **no practical benefit** to the recipient or the user."*	The purpose of this proposed amendment is to introduce an **exception** to the obligation to ensure **data portability** under **Chapter II of the Data Act** in situations where such data are **unreadable** or would provide **no practical benefit** to the recipient or user. At present, a significant proportion of the data that data holders may be required to share under Chapter II would not be understandable or legible to users or recipients, and their disclosure would bring no tangible advantage. Nevertheless, data holders are still required to incur costs to develop solutions enabling the sharing of such data. The proposed amendment therefore aims to **reduce the burdens** imposed on data holders by this obligation.
Abolish the prohibition under Article 5(3) for gatekeepers: *"3. Any undertaking designated as a gatekeeper, pursuant to Article 3 of Regulation (EU) 2022/1925, ~~shall not be an eligible third party under this Article and therefore shall not:~~* *(a) solicit or commercially incentivise a user in any manner, including by providing monetary or any other compensation, to make data available to one of its services that the user has obtained pursuant to a request under Article 4(1);* *(b) solicit or commercially incentivise a user to request the data holder to make data available to one of its services pursuant to paragraph 1 of this Article;* *~~(c) receive data from a user that the user has obtained pursuant to a request under Article 4(1).~~*	The amendment seeks to **abolish the absolute prohibition** on **gatekeepers**, as defined under the **Digital Markets Act (DMA)**, set out in **Article 5(3) of the Data Act**. This prohibition raises serious legal concerns due to a possible **conflict with Article 20 of the GDPR** and **Articles 6(9) and 6(10) of the Digital Markets Act**. In any case, a complete ban is inappropriate, as there may be situations in which users wish to share their data with a gatekeeper. The objectives of these provisions can be effectively achieved through a ban on gatekeepers soliciting or incentivising users to provide such data. See also the additional comments submitted by the CCIA to the European Commission and by the EDPB

Simplification #3: **Limiting the Obligations for Data Sharing by Enterprises with Public Sector Bodies (B2G) under Chapter V Exclusively to Product Data and Data from Related Services**	
"Art. 14 Obligation to make data available on the basis of an exceptional need. *Where a public sector body, the Commission, the European Central Bank or a Union body demonstrates an exceptional need, as set out in Article 15, to use certain data from a product or from a related service, including the relevant metadata necessary to interpret and use those data, to carry out its statutory duties in the public interest, data holders that are legal persons, other than public sectors bodies, which hold those data shall make them available upon a duly reasoned request.* *Art. 15 Exceptional need to use data* *1. An exceptional need to use certain data data from a product or from a related service, within the meaning of this Chapter shall be limited in time and scope and shall be considered to exist only in any of the following circumstances:* [...] *b) in circumstances not covered by point (a) and only insofar as non-personal data is concerned, where:* *i) a public sector body, the Commission, the European Central Bank or a Union body is acting on the basis of Union or national law and has identified specific data from a product or from a related service,, the lack of which prevents it from fulfilling a specific task carried out in the public interest, that has been explicitly provided for by law, such as the production of official statistics or the mitigation of or recovery from a public emergency; and* *ii) the public sector body, the Commission, the European Central Bank or the Union body has exhausted all other means at its disposal to obtain such data from a product or from a related service, including purchase of non-personal data on the market by offering market rates, or by relying on existing obligations to make data available or the adoption of new legislative measures which could guarantee the timely availability of the data."* [...]	The amendment aims to **limit the application** of **data-sharing obligations** in **B2G relations**, as set out in **Chapter V**, exclusively to **product data** (as defined in Article 2(15)) and **related service data** (as defined in Article 2(16)). The purpose of this change is twofold: (i) to ensure clarity and legal certainty regarding the scope of requests made under Chapter V, and (ii) to restrict the subject matter of such requests solely to product data and related service data. This amendment is intended to significantly reduce the operational burden associated with receiving and processing such requests, as systems and procedures could be implemented specifically within product-related domains, thereby streamlining the entire process.

Establishment of a list of entities authorised to submit requests under Chapter V *"Art.2 p. 27 'Union bodies' means the Union bodies, offices and agencies designated by the Commission in accordance with Article 23(1), set up by or pursuant to acts adopted on the basis of the Treaty on European Union, the TFEU or the Treaty establishing the European Atomic Energy Community* *Art.2 p. 28 'public sector body' means bodies designated as such by the Member States in accordance with Article 23(2); national, regional or local authorities of the Member States and bodies governed by public law of the Member States, or associations formed by one or more such authorities or one or more such bodies;"* New Article *"Art. 23* *1. The Commission shall be responsible for designating entities as Union bodies within the meaning of Article 2(27) and for maintaining a list thereof.* *2.The Member States shall be responsible for designating entities as public sector bodies within the meaning of Article 2(28) and for maintaining a list thereof."*	This amendment seeks to **require the Commission and Member States** to **establish and maintain lists of entities** authorised to submit requests under **Chapter V**. The purpose of this change is to ensure transparency and to prevent situations in which data holders could be overwhelmed by requests submitted by multiple entities that lack the legal right to make such requests under Chapter V.

II. ePrivacy Directive - cookies and other tracking technologies

Simplification of cookies & tracking rules - Harmonise and lighten ePrivacy Directive requirements on cookies and tracking technologies. Key amendments should exclude cookies used for contextual advertising, audience measurement or security from the consent requirement, as well as [remove the need for] cookie banners. Clarify that no banner is needed when consent is not required, which would reduce the number of cookie pop-ups and the associated "click fatigue" plaguing users. Additionally, resolve the conflict between ePrivacy and GDPR rules (consent vs. legitimate interest) for direct marketing, which currently breeds legal uncertainty and hinders the viability of many online services.

Detailed Recommendations – ePrivacy Directive

Simplification #1**: Extension of the Exception from the Consent Requirement under Article 5(3) of the ePrivacy Directive Regarding Cookies and Other Forms of Access to or Storage of Data on a Device for Security-Related Purposes**	
Proposed change	**Justification**
Amendment to Article 5(3) of the ePrivacy Directive and Extension of the Scope of Exceptions to Include Security-Related Cookies: *"3. Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access::* *a) solely for the purpose of carrying out the transmission of a communication over an electronic communications network; ~~or~~* *b) as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.;* *c) necessary to ensure or restore security, or to detect technical faults or errors in electronic communications networks or services (and related services or devices);* *d) necessary to detect or prevent fraud, abuse, or manipulation of electronic communications networks and services (and related services and devices) by the user, subscriber, or any other party, including in cases where such activities infringe upon the rights and legitimate interests of others or compromise the integrity of the network or service."*	**Benefits of adopting this recommendations** The proposed amendment aims to adapt the provisions of Article 5(3) concerning the processing of data on a device to the realities in which entities currently process data in the online environment. The existing rules are overly restrictive and create unnecessary barriers for many legitimate uses of cookies and similar technologies that have a low impact on privacy. Moreover, the current legal framework results in the storage of, or access to, data on a device being subject to stricter rules than, for instance, cloud-based processing, despite technological development leading to the design of products and features that intentionally store data locally, precisely because such an approach is more compatible with privacy protection principles. The suggested addition of points (c) and (d) to Article 5(3) would make it possible to access or store information on the user's device (for example, through cookies) where this is necessary in legitimate circumstances, such as ensuring security, maintaining the functionality of a product, or detecting abuse and fraud, including cases where misuse or manipulation of a service infringes upon the rights or interests of other parties (for instance, customers relying on the service). This amendment would benefit both users and industry, as it would enable the secure provision of online services through local processing methods. Overall, these changes are intended to enhance legal certainty for entities operating in the digital environment (including SMEs), many of which rely on cookies or similar technologies to ensure the security of their services. From the user's perspective, more flexible consent requirements could lead to a reduction in the number of cookie banners and the associated

	"click fatigue" that currently troubles internet users. Clarifying the legislation would also help reduce legal uncertainty and disruptions within the internal market resulting from inconsistent interpretations of the existing rules by supervisory authorities.
Simplification #2**: Extension of the Exception from the Consent Requirement under Article 5(3) of the ePrivacy Directive Regarding Cookies and Other Forms of Access to or Storage of Data on a Device for Analytical Purposes**	
Amendment to Article 5(3) of the ePrivacy Directive and Extension of the Scope of Exceptions to Include Analytical Cookies: *Proposed amendment to Article 5(3):* *"c) necessary for measuring the use of online content or services.* *The concept of measuring the use of online content or services referred to in Article 5(3)(e) of this Directive includes the measurement of traffic on a website, application, or service in order to understand how that website, application, or service is used, provided that such measurement does not involve profiling users across different websites, applications, or services."*	**Benefits of adopting this recommendations** The proposed amendment aims to adapt the provisions of Article 5(3) concerning the processing of data on a device to the realities in which entities currently process data in the online environment. The existing provisions are overly restrictive and create unnecessary barriers for many legitimate uses of cookies and similar technologies that have a low impact on privacy. Moreover, the current legal framework results in the storage of, or access to, data on a device being subject to stricter rules than, for example, cloud-based processing, even though technological development has led to the design of products and functionalities that intentionally store data locally, precisely because this approach is more compatible with privacy protection principles. The proposed addition of point (c) to Article 5(3) and the corresponding recital aims to enable access to, or storage of, information on a device for data analytics purposes. Clearer and more flexible rules defining when such access or storage is permissible for analytical purposes would reduce barriers to innovation and limit the legal uncertainty arising from the current provisions. Overall, these changes aim to enhance legal certainty for entities operating in the digital environment (including SMEs), many of which base their business models on online advertising and other uses of cookie and similar technologies, whether for generating revenue, ensuring security, or improving service quality. From the user's perspective, more flexible consent requirements could lead to a reduction in the

	number of cookie banners and the associated "click fatigue" that currently troubles internet users. Clarifying the legislation would also help to reduce legal uncertainty and disruptions to the functioning of the internal market resulting from inconsistent interpretations of the existing regulations by supervisory authorities.
Simplification #3**: Extension of the Exception from the Consent Requirement under Article 5(3) of the ePrivacy Directive Regarding Cookies and Other Forms of Access to or Storage of Data on a Device for the Purpose of Displaying Contextual Advertising to Users**	
Amendment to Article 5(3) of the ePrivacy Directive and Extension of the Scope of Exceptions to Include Analytical Cookies: *Proposed amendment to Article 5(3):* *"c) necessary for displaying contextual advertising to the user.* *The concept of contextual advertising referred to in Article 5(3)(c) of this Directive means online advertising selected on the basis of data collected during a single session in which the user interacts with a website, application, or service. This may include the selection of an advertisement based on:* *(i) the content that the user is currently viewing;* *(ii) in the case of a search engine – the user's current query; and* *(iii) the device that the user is currently using".*	**Benefits of adopting this recommendations** The proposed amendment aims to adapt Article 5(3) of the ePrivacy Directive—which governs the processing of data stored on users' devices—to the current realities of data processing in the online environment. The existing provisions are overly restrictive, creating **unnecessary barriers** for many legitimate uses of cookies and similar **low-privacy-impact technologies**. Furthermore, under the current legal framework, storing or accessing data on a device is subject to stricter rules than, for example, cloud processing, even though technological development increasingly leads to the design of products and functionalities that **deliberately store data locally** as a **privacy-enhancing measure**. The suggested addition of point (c) to Article 5(3), together with a corresponding recital, seeks to allow access to or storage of information on a user's device for the purpose of displaying contextual advertising. Clearer and more flexible rules defining when such access or storage is permissible for contextual advertising would **reduce innovation barriers** and **mitigate legal uncertainty** created by the current provisions. Overall, the amendment aims to increase legal certainty for entities operating in the digital environment, including SMEs, many of which rely on **online advertising** and other cookie-based technologies to generate revenue. From the **user perspective**, more flexible consent rules could **reduce the number of cookie banners** and alleviate the widespread issue of

	"click fatigue" experienced by internet users. Clarifying these provisions would also help reduce legal uncertainty and market disruption caused by inconsistent interpretation of the current rules by supervisory authorities.
Simplification #4**: Clarifying that the Display of a Cookie Banner is Not Required Where One of the Exceptions Provided for in Article 5(3) Applies (i.e. Where User Consent is Not Required)**	
Addition of a New Article 5(4) to the ePrivacy Directive: "4. *Entities carrying out activities covered by Article 5(3) shall have the freedom to determine how the information referred to in that provision is presented in a clear and comprehensive manner.* *Providing clear and comprehensive information, as referred to in Article 5(3) of this Directive, does not require the use of so-called "cookie banners" for the activities covered by points [a)–e)] of Article 5(3), provided that the required information is presented in a notice that is easily accessible to the user. The information provided for the purposes of Article 5(3) should be comprehensive with respect to the purposes of the processing. It is not necessary to provide exhaustive information regarding cookies or other similar technologies used for storing or gaining access to information stored in the user's terminal equipment."*	**Benefits of adopting this recommendations** As with the previous simplifications, this amendment seeks to clarify the rules governing access to and storage of information on a user's device (in particular, the use of cookies) and to enhance legal certainty for entities operating in the digital environment. Many organisations, including SMEs, rely on cookies and similar technologies to ensure the security of their services or to improve them, for example through the use of analytics. Clarifying these provisions would help reduce significant legal uncertainty and mitigate internal market disruptions arising from the inconsistent interpretation of current rules by supervisory authorities. From the user's perspective, more flexible consent rules could reduce the number of cookie banners and the resulting "click fatigue" that currently frustrates internet users. In situations where consent is not required, burdening users with such notifications provides little real privacy benefit especially given that users can easily access the relevant information in a privacy policy or appropriate notice whenever they wish.
Simplification #5**: Clarifying that "Storing of Information or Gaining Access to Information Already Stored" Does Not Cover Temporary Storage or Information Exchanged as Part of an Ordinary Internet Connection**	
Amendment to Article 5(3) of the ePrivacy Directive to Clarify the Meaning (and Limits) of "Storage" and "Access": "*3. Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with*	**Benefits of adopting this recommendations** The purpose of the proposed amendment is to make it explicitly clear that information transmitted as part of the ordinary functioning of the internet (for example, under TCP/IP protocols) or by devices not intentionally directed towards a specific recipient or sender does not fall within the scope of Article 5(3).

Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.<u>The storage and access referred to in paragraph 3 shall not include temporary or short-term storage, nor operations that form part of the ordinary exchange of information with the terminal when the user or subscriber accesses an information society service."</u>	An overly broad interpretation of Article 5(3), which inadvertently captures data transmitted in the course of normal internet operations, does not serve the main objective of the ePrivacy Directive - namely, the protection of users' privacy. On the contrary, it poses several risks: (i) further increasing the number of everyday online interactions requiring consent, thereby leading to "consent fatigue" and diminishing user engagement with genuine tracking technologies; (ii) worsening the user experience within the EU, as users could be forced to make unrealistic decisions concerning consent for essential processes underpinning the operation of the internet ecosystem; and (iii) creating an almost complete overlap between the scope of the ePrivacy Directive and the GDPR in relation to all personal data collected in the online environment. Importantly, this also undermines the purpose limitation principle in the GDPR, which would otherwise permit the further processing of such data for compatible purposes.
Simplification #6**: Partial Repeal of Provisions on Direct Marketing**	
We propose a partial repeal of the ePrivacy Directive provisions on direct marketing by deleting Article 13(3), which concerns unsolicited communications. The GDPR would continue to apply to direct marketing insofar as it involves the processing of personal data. In addition, we call for the requirement to align national implementations of the ePrivacy Directive with these amendments.	**Benefits of adopting this recommendations** The provisions of the ePrivacy Directive on direct marketing were originally intended to protect individuals from unsolicited one-to-one communications sent by advertisers to their current or potential customers using their email addresses or phone numbers for marketing campaigns. However, the provisions on direct marketing under the ePrivacy Directive vary depending on how they have been implemented by Member States, resulting in a system that is both redundant and inconsistent with the GDPR. Under the GDPR, direct marketing is regulated by the lawful basis of legitimate interest (as stated in Recital 47), whereas under the ePrivacy Directive it requires consent. This inconsistency creates legal uncertainty and undermines the profitability of many online services.
Simplification #7: **Partial Repeal and Harmonisation of Provisions on Traffic Data**	
(1) We propose a partial repeal of the provisions by revising Article 5(1) and removing the reference	**Benefits of adopting this recommendations**

to "and related traffic data", as well as deleting Article 6, which concerns traffic data. (2) In addition, we call for the alignment of national implementations of the ePrivacy Directive with these amendments. (3) We also propose the harmonisation of the interpretation of data minimisation and purpose limitation to ensure consistency between the GDPR and related EU legislation.	Network-connected devices are essential for innovation in the EU, and modern vehicles are effectively computers on wheels that continuously collect and transmit data via built-in SIM cards (for example, for navigation, diagnostics, infotainment systems, emergency calls, etc.). This communication is often routed through mobile networks, which means that it generates traffic data within the meaning of the ePrivacy Directive.

Other relevant simplification proposals related to privacy – GDPR

1. The GDPR should be made genuinely risk-based in order to fulfil its objectives and provide greater flexibility in the application of its provisions.
    - Explicitly recognise, in a new Article, the principle of proportionality – in particular based on (1) the risks associated with data processing and (2) the burdens of ensuring compliance.
    - Introduce a proportionality analysis into the provisions governing data transfers, to provide greater flexibility for low-risk data flows.
    - Limit obligations arising from data access requests submitted by data subjects
2. Reduce the administrative burden associated with compliance.
    - Particularly in relation to risk assessments for legitimate interest: introduce a presumption that such an interest exists for types of processing listed on a "white list", granting the controller a wider margin of discretion.
    - Require less duplicative documentation.
3. Reduce burdens linked to the exercise of data subject rights.
    - Lessen the burden of responding to data subject requests by introducing exemptions based on "disproportionate effort".
    - Reduce the level of individual customisation of responses where feasible.
4. Narrow the scope of special categories of data.
    - Limit such categories to data that clearly and directly concern sensitive information (or from which sensitive data could potentially be inferred).
    - Introduce an exemption for publicly available data, provided that appropriate safeguards are in place.
5. Improve the data transfer regime.
    - Simplify intra-group data transfers carried out in the course of ordinary business operations by recognising a presumption of adequate safeguards where the company self-certifies compliance.

- Allow greater flexibility in assessing third-country laws in the absence of an adequacy decision, including by taking into account the actual likelihood of public authorities accessing EU personal data.

6. Clarify the conditions for joint controllership.
7. Amend the mandate of data protection authorities under the GDPR to explicitly recognise economic and innovation interests and to provide clarity regarding the necessary balance between data protection and other rights and interests.
8. Strengthen the balance between the right to privacy and other fundamental rights and related interests.

III. Cybersecurity incident reporting

A single EU-wide reporting mechanism - unify and streamline cybersecurity incident reporting obligations across all EU laws. Today, a single incident can trigger reporting under multiple regimes (GDPR, NIS2, DORA, CRA, AI Act, etc.), each with different criteria, deadlines and authorities, meaning the same incident might need reporting in up to 27 Member States via various forms and tools. These duplicative, inconsistent and complicated reporting requirements divert key resources away from actual incident response without appreciable security benefit. We call for one EU-wide reporting mechanism" a single portal and template form managed by a designated EU authority for all such incidents. Core reporting elements must be harmonised (common incident definitions, aligned thresholds and deadlines - e.g. a standard 72-hour timeline) and a *report once, comply with multiple obligations principle* adopted so that one notification fulfills all overlapping legal requirements. A simplified and harmonised reporting process would allow entities to **focus more effectively on responding to incidents.** This would lead to faster recovery from security incidents, reduced harm to users and services, and, ultimately, a more resilient and secure digital ecosystem across the European Union.

Other relevant simplification proposals related to security

Simplifying Market Access Certification (Radio Equipment Directive, Cyber Resilience Act, European Cybersecurity Certification Scheme Based on Common Criteria, Data Act)	
Proposed change	**Justification**
(1) **Timely publication of standards:** Harmonised standards should be published at least 12 months before the date of application of the regulation. If the standards are not ready, the date of application should be postponed accordingly. (2) **Smooth transition pathways:** The transition from the RED to the CRA should include a clear mechanism under which devices certified under the RED could be automatically recognised or provisionally approved. For such	The current and upcoming product certification regimes create numerous challenges for manufacturers. For instance, under the Radio Equipment Directive (RED), harmonised standards have been published too late, forcing companies to conduct testing based on future, rather than applicable, standards. Furthermore, RED presents difficulties by linking hardware certification to software release timelines. Software is analysed much closer to the product's market launch, whereas

devices, compliance with the CRA should focus on verifying the manufacturer's secure product lifecycle management — the main distinction between the RED and the CRA. (3) **Recognition of industry certification schemes:** Established industry certification programmes should be recognised as demonstrating compliance with regulatory requirements. Notified bodies could maintain their supervisory role; however, test reports issued under recognised industry certification schemes should also be accepted. For example, it would be beneficial to recognise the GSMA Mobile Device Security Certification (MDSCert) scheme, based on ETSI standard TS 103 732-1 ("Consumer Mobile Device Protection Profile"), as sufficient evidence of compliance in the field of mobile device security. (4) **Recognition of international standards:** The European Union should make greater use of existing international standards rather than creating new European ones, which may lead to additional compliance requirements, trade barriers, and delays in the implementation of technical solutions and the achievement of regulatory objectives. (5) **Separation of hardware and software certification:** For devices such as phones and tablets, it is essential to separate the hardware and software certification processes under the RED (and, where applicable, the CRA) so that they correspond to actual product development cycles.	hardware certification is required before production begins — leading to significant scheduling discrepancies (for example, a three-month gap during which hardware teams require RED certification while software development is still ongoing). In relation to the forthcoming Cyber Resilience Act (CRA), the lack of available harmonised standards limits preparatory work. Moreover, some provisions, such as the proposed five-year minimum support period, may prove unfeasible for certain product categories (for example, wireless earbuds). There is also a need for clarity as to whether pre-installed applications on devices such as phones, tablets, and televisions will require separate certification. More broadly, regulations such as the EU Data Act would benefit from better alignment with existing standards and certification schemes. This alignment is essential to ensure that development teams clearly understand what is expected of them and can rely on third-party testing to verify compliance. These issues have tangible negative consequences, including substantial operational costs. Product development schedules are disrupted, and both legal and operational uncertainty increase. The potential need to re-test all devices under the CRA, despite their prior certification under RED, would impose a significant burden on the industry, with limited evidence of any real improvement in product security. The proposed changes would provide the predictability necessary for effective product development, which typically begins 12 months before market launch. Clear and timely requirements are vital for planning resources and functionality. Recognising industry certification schemes could help bridge the gap between broad regulatory language and specific engineering requirements, as such schemes often include detailed test plans and acceptance criteria tailored to particular product categories. This approach would reduce duplication of effort, lower compliance costs, and

	allow industry players to focus their resources on genuinely improving product security — ultimately benefiting both consumers and businesses within the EU.
Optimising Cybersecurity Management	
(1) Use of international standards: Encourage the application of existing, globally recognised security frameworks (such as ISO 27001 or ETSI EN 303 645) as reference points for demonstrating compliance with EU cybersecurity management requirements, rather than creating new, separate obligations applicable only to EU entities. **(2) Limiting inconsistent national systems:** Actively discourage Member States from adopting national cybersecurity certification schemes that diverge from the EU's harmonised approach or recognised international standards. **ENISA** could play a stronger role in promoting such harmonisation.	**Benefits of adopting this recommendations** Anchoring EU requirements in widely adopted international standards facilitates cooperation in global markets, reduces costs and obligations for internationally operating businesses, and allows them to build on previously implemented security measures. This approach ensures that resources are directed towards genuine security enhancement, rather than navigating a fragmented and duplicative regulatory landscape. **Risks of inaction** A range of EU legislative acts, such as the **NIS2 Directive**, the **Cyber Resilience Act**, the **Regulation on Digital Operational Resilience**, the **Cyber Solidarity Act**, the **Cybersecurity Act**, and the **GDPR**, **together create a complex landscape of requirements for cybersecurity management, coordination, and cooperation.** Although these measures are designed to improve security, the proliferation of overlapping obligations can result in ambiguity and administrative burden — particularly where they duplicate well-established international security frameworks (for example, ISO 27001). Moreover, the possibility for individual EU Member States to introduce their own, inconsistent cybersecurity certification schemes adds yet another layer of complexity. Unclear or overlapping cybersecurity management requirements impose a significant administrative burden on businesses. This burden often fails to translate into tangible improvements in security, particularly when resources are diverted towards demonstrating compliance with multiple overlapping regulatory frameworks rather than implementing robust protective measures.
Strengthening ENISA's Role in Shaping EU Policy	
(1) Independent security impact assessment for EU tech policy regulations: Just as the EU conducts impact assessments	**Risks of inaction** Regulations concerning technology policy — even when not directly focused on cybersecurity — can

for new initiatives in areas such as the economy, society, and the environment, it should also carefully assess whether new technology policies could pose risks to the security and privacy of citizens. A revised **Cybersecurity Act** should give **ENISA** a clear and strengthened role as an impartial body responsible for assessing proposed EU technology regulations. ENISA could prepare a "security impact assessment" for such initiatives, thereby improving the legislative process and delivering better outcomes for citizens. Providing policymakers with a dedicated security impact assessment, prepared by a specialised institution such as ENIS, would enable a better understanding of the potential negative effects of proposed regulations on the EU's digital security ecosystem and allow these risks to be mitigated more effectively. This would ensure that new legislation achieves its primary objectives without exposing users to unintended security or privacy threats. **(2) Aligning ENISA's mandate with its resources:** ENISA plays a vital role within the EU's cybersecurity ecosystem, supporting the implementation of regulations such as the **NIS2 Directive** and the **Cyber Resilience Act** by providing independent technical expertise, sharing best practices, consulting with the private sector, and assisting organisations of all sizes. Any revision of the **Cybersecurity Act** must strengthen ENISA's mandate as an independent, technical, and advisory authority, while also providing it with additional resources to support its expanding mission. For example, ENISA currently plays an important role in coordinating joint activities with industry through the **Cyber Partnership Programme (CPP)**. The CPP supports ENISA's mission of enhancing Europe's resilience to cyber threats by facilitating the exchange of threat intelligence between technical experts, which in turn informs policy planning and the	have a broad and far-reaching impact on the safety of EU citizens and the digital services they use. Compliance with various pieces of technology legislation, including the Artificial Intelligence Act and the Digital Markets Act, may in some cases unintentionally weaken existing protection mechanisms that businesses have already implemented. The need to comply with several distinct legal acts can lead to situations where design choices aimed at ensuring product safety and integrity must be modified in ways that introduce new risks or weaken existing safeguards. Security should be taken into account at every stage of the legislative and regulatory process in order to guarantee digital safety for all.

development of alerts for European businesses. ENISA must be equipped with sufficient resources and funding to continue running programmes such as the CPP, while maintaining its essential mission in the field of cybersecurity certification.	

IV. AI Act Implementation

Implement the AI Act in a pro-innovation, cohesive manner - refocus the AI Act on a proportionate, risk-based approach that is easy to implement and consistent across the EU. As currently designed, the Act risks fragmenting the single market: its flexible enforcement structure has led one Member State to plan nine different national AI regulators, and if every country followed suit there could be over 240 such authorities, creating an unprecedentedly complex oversight and enforcement system that would overwhelm administrative capacities. Unlike prior digital laws, the AI Act lacks a one-stop-shop or country-of-origin principle, complicating cross-border compliance. We urge the adoption of a swift EU-wide mechanism for cross-border case resolution and oversight coordination. Moreover, The Act's original purpose *was never to regulate the technology itself, but to focus on specific high-risk applications*. Provisions imposing broad obligations on general-purpose AI (GPAI) deviate from that aim. The Act should return to its original goal of regulating high-risk AI use cases, and the section that unnecessarily regulates AI technology, namely Chapter V and its recitals should be removed. Concretely, computing thresholds that trigger requirements on AI models should be raised (many current models already exceed the proposed values), with a roadmap to shift toward capability-based criteria in the future. Obligations for model changes should scale with the significance of the change - fine-tuning a model should incur compliance duties only if it materially alters the model's risk profile. These adjustments will ensure the AI Act *supports trust and innovation* by being **more risk-based, proportionate, up-to-date and feasible to implement**.

Detailed Recommendations – AI Act

Simplification #1**: Adopt a proportionate, risk-based approach to AI model fine-tuning**	
Proposed change	**Justification**
Adopt a proportionate, risk-based approach to fine-tuning (through AI Office guidelines or implementing acts):. **(1) Recognition of existing regulations:** It should be acknowledged that risks are primarily managed either by the original provider or, at	**Benefits of adopting this recommendations** It directly supports the EU's competitiveness and innovation by avoiding disproportionate burdens on potentially hundreds of thousands of entities operating further along the supply chain. It ensures that regulation remains targeted, risk-based and

the AI system level, by the entity performing the fine-tuning. The provider of the original general-purpose AI model should not be held responsible for compliance in relation to a model modified by a third party, apart from the obligation to provide documentation enabling that third party to operate lawfully. (2) **Classification of modifications:** Modifications should be classified according to their technical nature, rather than by the entity carrying them out. For modifications made at a later stage (forks), the computational threshold should apply equally to all entities - both internal and third parties - ensuring a level playing field and focusing on the significance of the changes introduced. (3) **Clarification of the possibility to rebut presumptions:** Model providers should have the ability to challenge the classification of a modified model as a general-purpose AI model by demonstrating that the final integration of the model within an AI system serves only a narrowly defined set of tasks, or that the capabilities significantly improved through modification do not correspond to the general-purpose nature of the original model. (4) **Template for summary updates:** The summary template should not apply to new models created as a result of modifications, and updates to summaries of general-purpose AI model versions should be presented in descriptive form. Furthermore, *de minimis* modifications, or those that do not cause a "significant change in the overall nature and capabilities compared with the original model", should not require an update of the summary template — even when performed by the original provider of the general-purpose AI model. (5) **Introduction of graduated obligations:** a) **Limited obligations** – apply only when a fine-tuned model (without significant changes) is made directly available to third parties (e.g. updating technical documentation, providing supplementary documents). b) **Full obligations (rare cases)** – apply solely in instances of "significant" fine-tuning, where	proportionate, in line with the original intent of the Artificial Intelligence Act. It provides legal certainty for entities engaging in model fine-tuning and recognises the existing regulatory frameworks at both the base model and AI system levels. It enables companies, particularly SMEs, to fine-tune models for specific, often low-risk applications without incurring the high costs already borne by general-purpose AI model providers. **Risks of inaction** A significant expansion of the regulatory scope could hinder the deployment and development of AI within the EU economy, as adapting general-purpose AI models may become overly burdensome, reducing their usefulness and uptake by businesses. This would have a disproportionately negative impact on SMEs and on the EU's competitiveness compared with entities using ready-made models or operating outside the Union. It would also create legal uncertainty that discourages investment and innovation, while undermining the focused, risk-based nature of the regulation.

elements prepared by the original provider may be reused. c) **No additional obligations** – apply when fine-tuning is carried out exclusively for internal use and is not significant in nature.	
Simplification #2: **Limitation of the territorial scope of copyright-related obligations, in particular with regard to exemptions for text and data mining**	
(1) Limitation of the territorial scope of Article 53: clarify that the obligations arising from Article 53 apply solely in cases where an activity falls within the scope of Union copyright law (e.g. placing a product on the EU market), in line with the principle of territoriality. Measures set out in the codes of practice for general-purpose AI models should explicitly include the phrase *"where applicable."* The substantive provisions of EU law should not be extended to cover model training conducted outside the Union's territory. **(2) Alignment of policy with existing legislation:** ensure that policy requirements relating to copyright (Article 53(1)(c)) are fully consistent with current copyright law and do not exceed its legal boundaries. Compliance obligations should not be imposed at earlier or later stages of the supply chain that fall beyond the provider's control. **(3) Clarification regarding text and data mining and Robots.txt:** focus on achieving consensus or standardisation of rules governing reservations on the use of data for training general-purpose AI models, while avoiding interpretations that would encompass all website indexing or conflict with search engine functionalities.	**Benefits of adopting this recommendations** It ensures legal certainty while respecting copyright law, reduces compliance challenges for globally developed AI models, facilitates access to a diverse range of models, supports innovation by focusing on market retention within the EU, and prevents unintended consequences for the wider internet ecosystem. **Risks of inaction** Ongoing legal disputes; significant legal uncertainty for global AI developers seeking access to the EU market; difficulties in enforcing regulations within the Union; technical complications if providers were required to retroactively apply EU opt-out mechanisms to training activities that were lawful in their original jurisdictions; substantial regulatory burdens hindering market entry; limited model availability within the EU; stagnation of innovation due to concerns over data acquisition and the need to retrain models; and a potential negative impact on the broader functioning of the internet ecosystem.
Simplification #3: **Review of Computational Thresholds for General-Purpose AI Models and Systemic Risk Models**	
(1) **Increase the computational thresholds** to **10^{23}** for **general-purpose AI models** and to **10^{26}** for **general-purpose AI models with systemic risk**. (2) **Define modification thresholds** in relation to the **actual computational power** of the base model (e.g. one-third of the computations of the original general-purpose AI model), rather	**Benefits of adopting this recommendations** An immediate reduction of regulatory burdens for models below the 10^{26} FLOPs threshold, allowing resources to be focused more effectively and aligning with the EU's regulatory simplification goals. Linking modification thresholds to the base model's computational capacity ensures consistency and prevents market distortions by avoiding disincentives for using high-performance

than applying a fixed, model-independent threshold. (3) **Develop a roadmap** outlining how these thresholds will be **progressively complemented or replaced** by a **capability-based assessment**, ensuring resilience to future technological developments.	models. Incorporating a roadmap towards capability-based assessments guarantees that the regulatory framework remains relevant and effective as AI technology evolves, reducing the need for frequent, reactive legislative updates. The proposal is consistent with international approaches, politically feasible, and provides a practical transitional solution acknowledging the limitations of current compute-based metrics until capability-based methodologies are mature. It also covers the next generation of models (assuming continued scaling of pre-training) without over-focusing on currently known or tested systems, and reduces administrative burdens for the European Commission. **Risks of inaction** Continued **misalignment of regulatory scope** based on an **outdated computational metric**. Potential **unfair market practices** due to loopholes linked to low compute thresholds. Possible **security gaps** if high-capability models remain **outside the scope** of regulation.
Simplification #4: **Streamlining the Self-Assessment Process for High-Risk AI Systems**	
(1) **Accelerate the publication of Commission guidance:** The Commission should issue its guidance well before the February 2026 deadline. This guidance must provide clear, objective, and practical criteria for assessing *"significant risk"* and *"substantial impact on decision-making"*. It should include specific examples of systems likely to qualify for exemption, for instance, those performing narrow procedural tasks, supporting prior human actions, or carrying out preparatory functions without replacing human judgement. (2) **Maintain provider self-assessment:** The process should be structured so that a documented self-assessment conducted by the provider in good faith and on the basis of clear criteria set out in the Commission's guidance constitutes sufficient justification for applying the exemption provided for in Article 6(3). Any potential regulatory review should focus on evaluating the adequacy of the documented self-assessment against those	**Benefits of adopting this recommendations** It provides legal certainty, enabling providers to apply the exemption in a justified and informed manner. It ensures that the risk-based approach established under the AI Act operates as intended, preventing disproportionate burdens on lower-risk systems. The proposal supports innovation by offering a clear and transparent pathway for deploying useful AI solutions in sensitive areas without unnecessary obligations linked to classification as a high-risk AI system. It also reduces administrative burdens associated with documenting assessments based on vague criteria and enhances **predictability** in product design and implementation. **Risks of inaction** Over-classification of systems as high-risk AI systems, hindering innovation in areas listed in Annex III due to concerns over compliance obligations. Significant resources may be **wasted on addressing ambiguities** and preparing

criteria, rather than disputing the provider's conclusions without presenting counter-evidence. (3) **Ensure proportionality of documentation:** The Commission's guidance should explicitly allow for the adaptation of documentation requirements to the context of the AI system. This should include the option of simplified formats where the absence of significant risk is clearly demonstrable based on well-defined criteria.	redundant documentation. Failure to act could **undermine the intended flexibility and proportionality** of the risk assessment framework established by the AI Act.
Simplification #5: **Revision of the Approach to Regulating General-Purpose AI (GPAI)**	
(1) Return to the original direction of the Act, ensuring a technologically neutral and risk-based framework focused on mitigating actual risks rather than regulating specific technologies. (2) **Remove Chapter V and its accompanying recitals from the AI Act.**	**Benefits of adopting this recommendations** The current regulatory framework for General-Purpose AI (GPAI) models poses significant challenges not only for providers but also for organisations that use, adapt, or deploy such models. By imposing restrictive obligations, the EU risks stifling innovation and operational efficiency, preventing organisations from leveraging AI technologies at the same level as their global competitors. This regulatory complexity affects not just individual entities but the EU economy as a whole, creating barriers to technological progress and market competitiveness.
Simplification #6: **Adoption of an Efficient Mechanism for Handling Cross-Border Cases**	
Chapter VII of the AI Act should be reassessed to include an improved mechanism for the resolution of cross-border cases.	**Benefits of adopting this recommendations** The flexibility of the AI Act regarding the designation of national regulatory authorities has led to proposals for the establishment of multiple bodies with varying expertise across Member States, which significantly complicates matters for businesses operating across borders. Without a dedicated mechanism for cross-border cases, several regulatory authorities in different countries could potentially claim jurisdiction over the same case. **Risks of inaction** This could result in an unstable regulatory environment for cross-border issues, making it more difficult for companies to operate within the EU. It could also lead to a situation where AI regulatory authorities are not required to maintain an appropriate balance between fundamental rights and other regulatory objectives, such as competition, innovation, privacy, and security.

V. Conclusion

Europe's digital future depends on regulations that are effective, proportionate, and innovation-friendly. The simplifications proposed in this paper aim to streamline the EU's digital frameworks, eliminate overlapping or contradictory obligations, and focus compliance efforts where they truly enhance security, trust, and most of all competitiveness. We urge EU policymakers to incorporate these proposals into the upcoming Omnibus legislative proposal. By doing so, the EU will send a clear signal that it is committed to upholding high standards while removing unnecessary red tape. This balance is essential to ensure that businesses of all sizes can thrive in the Single Market. Importantly, simpler rules will also benefit citizens and end-users, who will enjoy strong protections implemented in a more transparent and user-centric manner (fewer pointless notices, faster digital services, and more reliable safeguards where it truly matters).

About BSP

Business & Science Poland (BSP) combines the experience of leading Polish enterprises with the EU agenda. We represent the knowledge and interests of Polish companies employing over 180,000 people in Poland, the EU, and globally. Our goal is to support the EU Single Market in line with the need for its responsible and effective transformation. This opinion presents the position of BSP members representing the digital, financial, air transport, fertiliser, chemical, mining, refining, fuel and energy sectors.

Rue Belliard 40, 1000 Brussels
e-mail: info@zpbsp.com
EU Transparency Register Number: 548212735276-89