

GDPR	Challenge description	Suggested improvement
<p>Art 4, Definitions</p>	<p>The broad definition of personal data in Article 4(1) of the GDPR makes it difficult to know with certainty whether the processing in a specific case falls outside the scope of the GDPR or not. For example, the data controller often faces difficulties in gathering a proper overview of the available datasets and methods that other actors may use to identify a particular person.</p> <p>True anonymisation is difficult or even impossible to achieve and often reduces the quality and usefulness of data. To be innovative, competitive, and promote more AI development and use, companies need to be able to extract aggregated knowledge at group level.</p> <p>The current legal situation is too restrictive to foster innovation in this regard. If the broad definition of personal data is to be maintained, the requirements for legal basis and purpose limitation must be alleviated to ensure businesses' ability to use data for technology and AI development.</p> <p>The broad definition of personal data also impacts other use cases, such as camera surveillance via intercoms where no video footage is stored. The camera is basically just a peephole, but due to its digital camera the GDPR becomes applicable, and the controller thereby has to</p>	<p>We propose that the GDPR would not be applied to the processing of personal data, if the processing is temporary and if the purpose of the processing is unrelated to the data subject (see Prof. Wendehorst's '<i>non-personal use of personal data</i>' proposal in the link provided in reference.¹⁾</p> <p>It would be good if the Commission could consider whether an update to the definition of personal data is called for and if anonymisation could be better defined to clarify what has to be done to achieve it.</p> <p>For example, the EDPB's 2024 opinion on AI models⁸ indicates that the training of an AI model, including its outputs, may involve personal data, and that DPA's should evaluate on a case-by-case basis whether an AI model maintains sufficient anonymity.</p> <p>Currently, the EDPB 's guidance lacks consistency for businesses and is likely to lead to fragmented interpretation among Member States and is therefore likely to slow down the ethical development of AI models in the EU.</p>

¹ (see prof. Wenderhost's "*non personal use of personal data*" proposal here [Draft AI Data Protection Regulation WENDEHORST 24-12-20.pdf](#))

	<p>fulfil e.g. the information requirements under Art. 13-14 GDPR.</p>	<p>CJEU´s ruling EDPs v SRB (C-413/23 P) settles when pseudonymised data is personal data. The Court´s ruling stated that it depends on who is looking at the data.</p> <p>According to CJEU:”Pseudonymised data must not be regarded as constituting, in all cases and for every person, personal data for the purposes of the application of GDPR. It follows from the provisions of that regulation as interpreted in case-law that pseudonymisation may, depending on the circumstances of the case, effectively prevent persons other than the controller from identifying the data subject in such way that, for them, the data subject is not so longer identifiable.”</p> <p>Although the ruling provides greater clarity, it would be essential for competitiveness to introduce clear changes also to the GDPR itself.</p>
<p>Art 5 Principles relating to processing of personal data, Purpose limitation</p>	<p>Purpose limitation principle: Repurposing data for product and technology development, including training of AI models, is challenging under the current purpose limitation principle.</p> <p>In addition, the application of the accountability principle, and the lack of a true risk-based approach in this regard, entails a very heavy documentation burden on businesses. The current application of the</p>	<p>To ensure commercial companies' access to data, further processing of de-identified/pseudonymised data for product and technology development must be considered a compatible purpose (not just in the context of research). This should be explicitly stated in the recitals of the GDPR or in Art. 5(1)(b).</p> <p>To avoid unnecessary documentation burden on businesses, art 5 (2) should be changed to emphasize that no or less documentation is needed where privacy</p>

	<p>accountability principle (and related enforcement) results in companies conducting a large amount of documentation purely for auditing purposes, with no real impact on individual's data protection.</p>	<p>risk is low (also referencing article 24 on the risk based approach).</p>
<p>Art 6, Lawfulness of processing</p>	<p>Processing of personal data for product and technology development (AI included), is currently too restricted. In practice, it is rarely feasible to base such processing on consent. At the same time, it is often uncertain whether other, more appropriate, legal bases such as legitimate interest (the balancing of interests) would apply. Of course, the need to carry out a legal assessment on a project-by-project basis cannot be completely removed. However, from a broader perspective, the current legal situation appears overly uncertain and restrictive to foster innovation.</p>	<p>As a solution, we propose clarifying the legal grounds for processing personal data. Legitimate interest and contract are the most important and widely used legal bases for companies' data processing. Their application should be straightforward in ordinary, low-risk situations. For processing of pseudonymised data for technology and AI development, the main rules should be that a company's interest shall prevail. The possibility to rely on contractual processing should be broadened. The balancing test required for legitimate interests should, in most cases, be unnecessary, and this should be explicitly stated in the regulation.</p>
<p>Art 9, Processing of special categories of personal data</p>	<p>Processing of special categories of personal data (SCD), (i.e. racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union memberships, health, or sex life or sexual orientation, as well as genetic or biometric data processed for the purpose of uniquely identifying an individual). Processing of SCD is prohibited, unless any of the exemptions in Art. 9 GDPR is applicable (e.g. that the data subject explicitly consents to the processing, the processing is necessary for the establishment, exercise or defense of legal claims or the processing relates to personal data which are manifestly made public by the</p>	<p>The restrictions for processing SCD should pertain solely to data processed with the intent of revealing such data. It should also be clarified that "revealing" does not mean the existence of any theoretical possibility of identifying a sensitive trait.</p> <p>There is no legal basis like the legitimate interest when processing SCD, which puts an unnecessary limit on the processing of such personal data where the processing would be needed e.g. to avoid bias and promote representativeness. A suggestion would be to add a legal exemption for processing of special categories of</p>

	<p>data subject). There is no legal basis similar to the legitimate interest to process SCD, which puts an unnecessary limit on the processing of such personal data where the processing would be needed e.g. to avoid bias and promote representativeness or where such data is a part of larger training data sets, but the connection to individuals is irrelevant to the processing.</p> <p>Processing of special category of personal data for technology, AI systems and models' development is currently extremely challenging. For large data sets it is impossible to rely on consent, and there are rarely other legal bases available. Large language models are for example developed based on enormous data sets collected by scraping the internet for content amongst other data sets. For development of AI-models and processing of very large data sets it is impossible to rely on consent, and therefore it is currently nearly impossible for commercial businesses to process special category data – even if highly de-identified – to train systems and models.</p>	<p>personal data, similar to the legitimate interest's basis in Art. 6 (1) (f) GDPR, to Art. 9 GDPR.</p> <p>Proposal: A new legal basis for processing special category data, Art 9:</p> <p>A new legal basis for processing special category data on a de-identified/non personal use of personal data should be introduced. An alternative could be a new and stricter legitimate interest assessment for special category of personal data.</p>
<p>Art. 13 and 14, Information to be provided to data subjects</p>	<p>Provision of information to individuals</p> <p>Part of the information obligations are too burdensome for companies to comply with and the little data protection it creates doesn't match the time spent. We need more proportionality in the current requirements.</p> <p>It is furthermore a challenge to provide information in cases where personal data is being collected without a</p>	<p>The extent of the information obligation under Art. 13 and 14 should be considered. We would like to see sub-articles 13(1)(d) and (f) and 13(2) (e) (and 14(1)(f) and 14(2)(b)) removed.</p> <p>Furthermore, we propose to underline in the preambles that only informing of categories of recipients is enough.</p>

	<p>direct relationship between the controller and the data subject.</p> <p>There are cases where publicly accessible personal data (including such that the individuals intentionally have made public) are processed, in a non-privacy sensitive manner, such as in the context of potential recruitment, identification of potential business partners, or mapping of gender equality in certain sectors. Such processing of personal data is, however, still subject to all requirements under the GDPR.</p>	<p>Lastly the area of application for Art. 14(5)(b) should be expanded, especially when the data in question is publicly available.</p>
<p>Art 15 and 12(5), Right of access by the data subject</p>	<p>Data subject access requests including the right to obtain a copy, are a large burden on companies, and automation of such requests are especially costly as they require sophisticated systems to ensure search and export of data across dispersed systems. The individual's right to data access should be limited to the data that is most informative for the individual, and more derived data with little meaning to the individual should be omitted. This means logs and metadata for example – where general information provided to the individual is sufficient, and – data access is of little to no value and an immense burden on companies. As digital services and infrastructures grow more complex, absolutist interpretations of Data subject requests obligations are out of step with real-world systems and constraints. The GDPR does not sufficiently consider the cost of meeting (often unnecessarily extensive) requests.</p>	<p>Consider revising Art. 15 so that controllers, in response to a broad access request,</p> <ul style="list-style-type: none"> (i) have the right to request reasonable clarifications of scope of access requests and – if none is given - deny the request, and (ii) should only be required to provide details of processing purposes and applicable legal bases as a first step, following which the data subject can choose what purposes it needs further information on. <p>The right of access should be exercised strictly for reasons of data protection and not be considered an absolute right. One way to address this issue could be to amend Art. 12 (5) GDPR, regulating manifestly unfounded or excessive requests. The EDPB Guideline on Right of Access needs to be updated to reflect the CJEU case law and provide for a right of access that</p>

	<p>Requests are often unrelated to the lawfulness of processing of personal data. Per the EDPB Guidelines on Right of Access, the overall aim of the right of access is to provide individuals with sufficient, transparent and easily accessible information about the processing of their personal data so that they can be aware of and verify the lawfulness of the processing and the accuracy of the processed data. A large amount of data subject requests that are received are not motivated by how privacy sensitive the processing activities are.</p> <p>Data subject rights are not seldom used for other purposes than those related to whether the processing of personal data is lawful or not. Instead, it is common that e.g., a request of access (Art. 15) is used for various strategic purposes, such as: to obtain information about a terminated employment; to gain advantages in a legal dispute or just to put pressure on the controller in some other context, e.g. to obtain negotiation leverage if the individual is unhappy with a product or service; or to gain competitive advantages, e.g., by way of monetising purchase history data from competitors.</p> <p>The GDPR does not sufficiently consider the cost to satisfy (often unnecessarily broad) requests. Data subjects are typically interested in how their personal data are processed in particular contexts. It is nevertheless easy to just request "all personal data that</p>	<p>reasonably satisfies the need to verify the lawfulness of the processing of personal data.</p> <p>The right of access to information about "recipients" of personal data should be changed to only include right of access to information about third party data controllers receiving personal data.</p>
--	--	--

	<p>are being processed about me" leading to unnecessary work for the controllers.</p> <p>Controllers spend a considerable amount of time determining what information or documents that should be produced and how these should be lawfully redacted. Many companies lack technical support to collect the data in an easy way and thereby risk not providing the data subject with all personal data that he or she has rightfully requested. Moreover, assessing limitations to and exemptions from the right of access is often highly complex and requires capabilities that many companies, and in particular SME, lack.</p>	
<p>Art. 22, Automated individual decision-making, including profiling</p>	<p>Art 22(1) prohibits automated individual decision-making in cases where the decision produces legal effects concerning a natural person or otherwise significantly affects them. However, the prohibition does not apply where automated decision-making is expressly permitted, for example, under other EU law or the national legislation of a Member State.</p> <p>AI systems are increasingly responsible for automated decision-making across various sectors, both private and public sectors.</p> <p>Furthermore, different interpretations from national DPAs on what is the correct legal basis for certain types of automated decision-making lead to legal uncertainty for companies engaged in AI development and usage. But</p>	<p>Consider modernising the EU-regulation. Remove the GDPR's regulation of automated decisions and let them be covered by the high-risk area of the AI Act (which they are already covered by to some extent today). Or improve legal certainty with a clarification of the connection between the GDPR's restrictions on profiling (Art 22) and the AI Act.</p>

	<p>also, slowing down AI pilots in the public sector hindering improved productivity by using AI to a larger extent.</p> <p>Annex III of the EU AI Act lists high-risk AI use cases. One such high-risk (but still permissible) use case concerns the assessment and decision-making related to essential private and public services and benefits.</p>	
<p>Art 24, Responsibility of the controller</p>	<p>The principle implementing appropriate measures according to risk is viewed by some DPAs as binary, making it difficult for companies to operate risk-based, when complying with all other articles of GDPR than 32-34. Data Protection Authorities or the EDPB do not take a risk-based approach sufficiently into account when auditing businesses or providing guidance. In essence it has the consequence that all processing activities is going through very extensive documentation, which we do not believe was the intent with the regulation. There are currently large amounts of GDPR documentation being produced, with little to no effect on individual's data protection.</p> <p>Responsibilities between controller and processor do not reflect the reality for businesses in situations where large platform services (in the role of processor) define the policies, and smaller businesses using the platforms (in the role of controller) have no real influence on the process.</p>	<p>Art 24 should be updated to further emphasise and acknowledge that all accountability measures (documentation requirements) taken by the controller should be risk based, also forcing data protection authorities to take this into account for auditing and guidance.</p> <p>We agree that there should always be a legal basis for processing personal data or that data should be erased in accordance with the principle of storage limitation.</p> <p>However, it is disproportionate to e.g. require retention policies and logs and documentation of all legitimate interests to ensure compliance with art. 24, cf. 6(1)(f) and 5(2) for all processing activities. Rather it should be sufficient for most processing activities – especially low and medium risk.</p>

Annex I, Nordic position paper, GDPR simplification

<p>Art 28, processor</p>	<p>Reviews of DPAs are burdensome, as many have different wordings and the need to document compliance with art. 28 thus becomes a checkbox exercise.</p> <p>Assessments of risks happens in the main contract, addendums and IT-security sections, knowing what the purpose of the processing is, what data is processed and when a processor becomes controller.</p> <p>Knowing the processing chains are often too burdensome in light of the risk of the processing and for processing with higher risk, knowing the chain is often just a checkbox list.</p>	<p>It should be possible to reference the requirements in art. 28 in a section of a main contract that often also already address the purposes. The security requirements could be regulated in a security addendum, which companies often have to comply with IT-security standards.</p> <p>Thus GDPR-compliance is centralized and fits better with existing processes when adding new suppliers.</p>
<p>Art 30, Records of processing activities, ROPA</p>	<p>The obligation to develop and maintain records of processing activities is limited to enterprises with more than 250 employees (proposal to increase threshold to 750 employees), however this does not apply when the processing carries high risk, which often is the case if it includes special category data. Since employers are processing special category data about their employees, and hence the requirement often still applies.</p>	<p>In addition to the proposed simplification, in order to lessen the administrative burden even further it would be beneficial to remove the requirement for all companies with no exemptions for certain processing (the requirement to make DPIA on high-risk processing and accountability principle and requirement to "demonstrate compliance" would still apply).</p>
<p>Art 33 Notification of data breaches</p>	<p>Reporting low risk data breaches entails an unnecessary administrative burden on companies and has no to little effect on individuals' privacy rights. In addition, it is resource-consuming for data protection authorities, and these resources are better spent more efficiently elsewhere on other tasks.</p>	<p>Breach reporting to national DPA's should only be done when the data breach is likely to result in . a high risk. Consider merging Art 33 and 34.</p> <p>The Commission should be given competence to introduce a common template for reporting across the EU. The report should be possible to fill in either in the</p>

	<p>As for what information that should be provided in the personal data breach notifications, there are big differences between EU countries. When dealing with a cross-border notification, complying with the obligation to notify the DPA within the 72 hours after becoming aware of the personal data breach is very challenging. The additional strain of trying to collect the different information for different DPAs is unnecessary and adds to the feeling that the GDPR is a nationally fragmented and complicated legislation.</p>	<p>member state's national language or English to support the internal market and reduction of administrative burdens.</p>
<p>Art 35 Data privacy impact assessment (DPIA)</p>	<p>DPIAS are cumbersome for businesses to conduct and review and are often very hard to integrate into business processes. A more flexible approach on how to conduct DPIA's would give companies greater room to integrate them into business processes and harvest the benefits that compliance gives.</p> <p>Furthermore, DPIA's are too often a requirement to do. DPAs seem to have an unnaturally low threshold on when a risk is high, leading to excessive use of DPIA's which can have an adverse effect when employees hardly find them necessary.</p> <p>The current interpretation and guidance on when and how to conduct a DPIA results in companies developing excessive documentation in number of DPIAs. This relates to the requirement to conduct a DPIA for each type of processing/each purpose and also in relation to what is considered high risk processing.</p>	<p>Ease the requirements for DPIA by removing the word 'systematic' and requirement to describe the legitimate interests from Art. 35(7)(a) and remove Art. 35(9) requirement or at least make it voluntary.</p>

<p>Art 44, 45, 46 General principle for transfers, Data transfers to third countries</p>	<p>Overall, the international transfer regime places an excessive burden on companies.</p> <p>The rules on international data transfers create unnecessary bureaucracy. The use of Standard Contractual Clauses under Commission Decision (EU) 2021/914 requires a transfer impact assessment, including an evaluation of the third country’s legal system, which leads to duplicative efforts by individual organizations. In some cases, such as transfers to third-country entities already subject to the GDPR under Art3(2), suitable transfer mechanisms are difficult to identify.</p>	<p>There is an urgent need for a risk-based framework from the EU Commission to lessen the burden away from individual companies, such as issuing more adequacy decisions or recommendations on adequacy level. The requirements to conduct Transfer Impact Assessments leads to companies wasting time on low-risk data processing activities, with no real impact on individuals’ data protection. The requirement to implement and document appropriate safeguards and if necessary supplementary measures, should be dependent on the risk of transfer. This risk-based approach should be reflected in the provisions or the preamble of the regulation.</p> <p>The Commission should take more decisions on the adequate level of data protection and assess the legality of data transfers by large players rather than individual companies.</p> <p>Legal certainty regarding the existing adequacy decisions and agreements on the level of data protection with key data transfer countries should be further developed and legal certainty about arrangements permanence should be increased.</p> <p>It would also be advantageous to simplify and consolidate the framework for data transfers based on EU’s SCCs and provide clarity on transfer effects.</p>
---	---	--

Streamlining the GDPR in relation to other EU digital regulation		
	Challenge description	Suggested improvement
GDPR and the AI Act	<p>The AI Act and the GDPR are different sets of rules, but they have many similarities and need to be applied together in their own areas. For high-risk AI systems, it is especially important that the two are aligned to make compliance possible. Applying them in parallel creates overlaps: some rules confirm that the GDPR comes first, some aim to match the AI Act with it, and others add to its rules.²</p> <p>It is crucial that the GDPR does not disproportionately hinder the EU's goal of becoming a global leader in AI development. To ensure that the EU regulation fosters trust and innovation, it must be refined into a more risk-based, proportionate framework that is future-proof and eases compliance.</p>	<p>For example, Art 59 of the AI Act defines when it is possible to deviate from the original purpose of personal data processing under the GDPR in a sandbox-environment during AI development. This is allowed if the AI model is being developed, for instance, to promote public health, public security, critical infrastructure, or the green transition. The scope of these exemptions should be clarified and expanded to also cover companies' own AI development needs.</p>
GDPR and the ePrivacy directive	<p>The ePrivacy Regulation proposed in 2017 was intended to replace parts of the ePrivacy Directive. As a regulation (Act), being directly applicable legislation, it would have taken precedence over national law and directives, thereby harmonising, among other things, cookie practices across the EU internal market.</p>	<p>The interaction between the ePrivacy Directive and the GDPR must be clarified to avoid overlapping obligations for companies.</p> <p>For example, Art 5(3) of the ePrivacy Directive relating to, among other issues, on cookie consent should be</p>

² Research by Uppsala University on the overlaps between the GDPR and the AI Act: [AI Data Governance : Overlaps Between the AI Act and the GDPR](#), pages 9–11.

	<p>However, the legislative process for the new ePrivacy regulation was delayed, which led the Commission to decide to withdraw the ePrivacy Regulation proposal in 2025.</p> <p>The ePrivacy Directive continues to be implemented in a fragmented manner across Member States, and it also contains certain overlaps with the GDPR.</p>	<p>repealed and incorporated into a GDPR-based solution, since cookies are primarily considered personal data.</p> <p>Such a solution would enhance legal certainty and reduce differences in how the directive is interpreted across Member States.</p>
<p>Art 14,15,12.5, 21 + DGA, Data Act, AI Act, CRA</p>	<p>Data subject rights request The protection of the fundamental right to data protection in the ever more digital world is a prerequisite for the trust and uptake of technology and breakthroughs.</p> <p>The Data Governance Act in that regard has potential to increase awareness and empower data subjects to exercise their rights in a way that is compatible with the GDPR. But the compliance with a data subject rights request might become even more challenging, and even more time-and-resource consuming, when it comes to connected products, under the Data Act, the AI Act, or under the Cyber Resilience Act (CRA).</p> <p>Furthermore, the CRA includes data minimisation essential requirement for products, whereas the AI Act would include requirement for recording the log data for transparency and traceability reasons.</p> <p>The Data Act, covering personal and non-personal data, raises concerns about clashing enforcement regimes and</p>	<p>Compliance with a data subject rights request will become even more challenging, and even more time-and-resource consuming, when it comes to connected products, under the Data Act, the AI Act, or under the Cyber Resilience Act (CRA).</p> <p>Therefore, it's highly recommended to consider (see above-mentioned proposals) amend Articles 14, 15, 12.5 and 21 of the GDPR.</p> <p>The seamless coordination of competent authorities in all those new legislations will be extremely important for the Single Market to ensure data-driven innovation and data protection.</p>

	<p>overall interplay with GDPR, questions pertaining to data minimization, and an increased need for being able to easily separate personal data from non-personal data.</p>	
<p>Incidents reporting/ Cybersecurity NIS2, CER Directive, CRA, GDPR</p> <p>(Directive (EU) 2022/2555 ; Directive (EU) 2022/2557 ; Regulation (EU) 2024/2847 ; Regulation (EU) 2016/679</p>	<p>These pieces of legislation inconsistently require entities to report incidents which have or can cause a disruption of the provision of the essential or important service. In a hypothetical situation where a physical intrusion/accident (CER-scope) in an energy sector entity, leads to compromise of data, integrity and authenticity of the service (NIS2-scope), the incident is reportable under those two laws, and if the compromise was a function of a publicly known exploited vulnerability of a product integrated in the system - a report of that is also due under CRA-scope (the entity notifies the manufacturer, which still requires a process and human resources allocation); and if personal data was breached the entity must report under the GDPR.</p> <ul style="list-style-type: none"> ○ NIS2 Directive requires Cybersecurity incidents to be notified within 24h and reported with more details 48 hours later (72) to the CSIRT, and vulnerabilities to be reported voluntarily. ○ Overlap with GDPR (EU) 2016/679: requires data breaches (which can be a result of cybersecurity incident subject to the reporting in NIS2 or in CRA) to be reported in 72h to the data protection authority. ○ Newly adopted Cyber Resilience Act, introduces reporting obligations of 24h to the 	<p>Implementation of the “once-only” principle. A clear instruction that a report of a significant incident to one of the competent authorities (whenever they do not overlap) is deemed sufficient and compliant with all those rules, should be introduced.</p> <p>In addition, the interim reports “upon request” by the competent authorities under incidents in the scope of CRA and NIS2 Directive should have the option to be refused by the entity, if there is no capability for an action to be taken by the competent authority to directly help the mitigation of the incident (only want interim report if you know you can act upon the information as a competent authority).</p> <p>The first step is to conduct a thorough mapping of these requirements and administrative setup with respective competences of the authorities in charge to understand the linkages between them as well as potential risks for inconsistencies, fragmentation and negative effects on dedicated resources.</p> <p>Streamlining and simplifying the requirements of the various regulations should be the next step. Compliance authorities are encouraged to make provision for synergies in the event of overlapping reporting</p>

	<p>competent authorities for an incident and/or vulnerability in a product (again potentially overlapping with a cybersecurity incident NIS2, that can also entail data protection breach, GDPR).</p> <ul style="list-style-type: none"> • Businesses of all sizes are confused with all the reporting requirements and their potential overlaps or reporting similar information several times to different bodies. Even if one legislation is addressed to entities (NIS2) and the other to processors and controllers (GDPR), or product manufacturers, some service providers (CRA) may overlap in certain cases: an entity can be a controller/processor; a manufacturer could also be a processor/controller; service provider being entity. All this will cost not only legal fees to understand the obligations, but also human hours to execute the different processes and respond to also ad-hoc requests (as NIS2 and CRA allow for authorities to ask companies to give updated information "upon request"). Businesses are afraid that resources inevitably will be diverted from the core mission of the cyber team, i.e. fixing the incident or vulnerability. 	<p>obligations in order to avoid unnecessary financial and administrative burdens and to ensure that the notification process runs smoothly and on time. Notification requirements should therefore be harmonized with regulatory frameworks, and a realistic notification timeframe should be defined, considering the operational realities of the entities involved.</p> <p>Perfect synergies between the competent authorities will ensure that exchanges of confidential information between authorities are limited to those cases strictly necessary to protect the commercial interests of companies.</p> <p>Clear instructions of what a critical product is must be analysed, considering the specifics of various industrial sectors/applications.</p>
<p>GDPR, AI Act, PWD Definitions</p>	<p>The AI Act, the GDPR and the Platform Work Directive have definitions respectively of “AI system”; “automated individual decision-making”; “automated monitoring and decision-making systems”; whereas the latter (the PWD definition) is redundant as it intersects the GDPR and AI Act provisions.</p>	<p>The EU Blue guide is a helpful tool to interpret EU product legislation, but it often transpires that even penholders do not necessarily know about the NLF principles, and the Blue Guide’s explanations. More streamlining and clarity could be achieved through:</p>

		<ul style="list-style-type: none"> • A centralized / domain glossary of standardized terms within the EU legal frameworks. • Mandatory cross-referencing of definitions when drafting new legislation. • A dedicated taskforce to review and align existing legislation.
<p>Transparency and reporting requirements for platforms Digital Services Act, AI Act, GDPR</p>	<p>Parts of the DSA's requirements for transparency, risk management, and oversight of algorithmic systems for digital platforms overlap with the AI Act's rules for high-risk and generative AI systems, as well as with the GDPR, where the latter is already established in terms of format and delivery of information to users.</p>	<p>Remove the redundant requirements and align the risk-based approaches of DSA and AI Act (e.g. Art14 DSA; Art 50 AIA).</p> <p>Amend the scope from algorithmic system in DSA to AI-system to align definitions with the AI Act and the requirements for transparency, risk management and oversight.</p>
<p>Use of algorithms in the workplace GDPR AI Act Platform Work Directive (PWD)</p>	<p>Three different regulations—AI Act, PWD, and GDPR—govern the same task allocation systems with differing logics: safety, fairness, and data privacy.</p> <p>Platforms face overlapping obligations (e.g., multiple impact assessments, transparency reporting to both workers and regulators, documentation under different regimes). This causes legal uncertainty, operational complexity, and innovation disincentives.</p> <p>GDPR already regulates much of what the PWD and AI Act seek to impose (e.g. right to explanation, data minimization, human oversight). However, the PWD introduces parallel rights that duplicate these GDPR obligations and could create interpretive conflict (e.g., stricter bans on biometric checks or data categories</p>	<ul style="list-style-type: none"> • Introduce cross-references between AI Act, GDPR, and PWD based on the once-only principle. • Establish a unified risk assessment framework acceptable under all three. • Encourage joint guidance from supervisory authorities (EDPB, AI Office, Labour Inspectorates). • Align AI Act requirements with existing GDPR principles and recognise sector-specific regulatory frameworks (like the PWD) to avoid double compliance for similar risk scenarios.

	<p>already addressed by GDPR). Furthermore, as the PWD will be transposed in 27 different ways, very different obligations on the use of algorithms may arise between the EU member states.</p>	<ul style="list-style-type: none"> • Limit prohibitions under art 7 • Align consultation requirements with the GDPR under Art 8 • Align the right to data portability: Art 9 with Art 20 of the GDPR • Align transparency requirements in Art9 with Art 22 of the GDPR • Limit the scope of Art 10 of PWD to the issue as dealt with Art 22(3) GDPR • Align the timescales under Art 11 with GDPR
<p>International (non-personal) data access and transfers</p> <p>Data Act, Data Governance Act GDPR</p>	<p>The General Data Protection Regulation Regime for personal data transfers provides for the identification of jurisdictions with which there is an equivalent protection of the fundamental right of data protection, and therefore personal data transfers could take place. The protection of fundamental rights should ensure that safeguards for both personal and non-personal data are in place, as it would be paradoxical for a jurisdiction to offer strong protection for non-personal data while neglecting the rights and privacy of individuals. Therefore, the provisions in Data Governance Act and in Data Act-would be costly for all sizes of companies (data holders, data processing services) to abide by the two parallel regimes (one for personal and mixed data sets, and one for all other data); and additionally, requiring businesses to assess the compatibility of third-country government data access requests with Union or national law imposes a complex and costly legal burden that could de facto</p>	<p>Delete the corresponding articles, i.e. Art 31 DGA and Art Art 32 Data Act.</p> <p>Introduce in the Data Act a clarification that countries considered having equivalent protection under the GDPR would be considered to have an adequate legal framework also for non-personal data transfers.</p>

Annex I, Nordic position paper, GDPR simplification

	<p>lead to data localization and disproportionately affect smaller economic actors, raising concerns of unequal treatment.</p>	
<p>Platform Work Directive GDPR</p>	<p>Art 8 of the Platform Work Directive requires a Data Processing Impact Assessment DPIA under Art 35 of the GDPR where algorithmic management tools are used. While the GDPR doesn't require DPIA to be shared publicly, the Platform Work Directive obliges digital labor platforms to proactively disclose DPIAs (which are very technical and complex documents) to platform workers and their representatives, which is de-fact two regimes for the same entity – one DPIA under GDPR and one for PWD's specific instance. The DPIAs will also be looked at by different authorities.</p> <p>Under GDPR (recital 63) data subjects' rights to access information must be balanced with other rights, e.g. intellectual property protection etc. and such balance should not result in refusal to provide information.</p>	<p>Remove the obligation to provide the DPIA to workers and their representatives; thus, keeping only the obligation under Art 12 of GDPR for transparent information to data subjects.</p>
<p>Data protection and financial crime compliance GDPR</p>	<p>Varying interpretations of data protection laws stand in the way of implementing financial crime compliance and fraud prevention measures in an effective and efficient manner.</p> <p>There are different types of data with different rules applying to data sharing for financial crime compliance and fraud prevention purposes. For instance, while it is desirable to share as much information on fraud events as</p>	<ul style="list-style-type: none"> Align fraud prevention and AML/CFT compliance measures in GDPR guidance or in separate laws that foresee an explicit deviation from the GDPR to improve clarity and ensure financial institutions can respond swiftly and effectively to emerging threats, i.e. not only limited to money laundering offences, but also sanctions avoidance, monetary fraud.

Annex I, Nordic position paper, GDPR simplification

<p>Anti Money Laundering /CFT</p>	<p>possible (e.g., fraudulent IBANs, location data, behavioural data), some EU and national rules restrict access to and sharing of sensitive data beyond Payment Service Providers (PSPs), notably to protect personal data (GDPR). Some fraud prevention measures may be limited to AML/CFT preventing pro-active sharing of fraud suspicion or fraud events. Yet other actors than Payment Service Providers could also play a key role in preventing fraud from spreading to other stakeholders and countries.</p>	<ul style="list-style-type: none"> Clarify that as a default option, fraud events data could be shared beyond the Payment Service Providers.
<p>Dark Patterns GDPR, Digital Service Act, Digital Markets Act, AI Act and the Unfair Commercial Practices Directive (UCPD)</p>	<ul style="list-style-type: none"> “Dark patterns” duplications and overlaps across various regulations and national transpositions, in particular the UCPD lead to a plethora of inconsistent terminology and requirements on how to deal with one and the same issue essentially. For example: Recital 32 of the GDPR, clearly describing that consent is an affirmative action, freely given and pre-ticked choices do not constitute freely given consent. Digital Services Act (DSA) – Article 25 addresses the use of dark patterns on online platforms. Digital Markets Act (DMA) - Recital 37 prohibits gatekeepers to design, organise or operate their online interfaces in a way that deceives, manipulates or otherwise materially distorts or impairs the ability of end users to freely give consent, which is in conjunction with obligations in Article 25 on data protection by design. 	<p>Do not propose new rules on dark patterns, as the current framework has a broad coverage.</p> <p>Create a cross-DG taskforce between the Units in DG JUST and DG CNECT responsible for monitoring the implementation of the relevant laws and include relevant stakeholders.</p>

Annex I, Nordic position paper, GDPR simplification

	<ul style="list-style-type: none">• Unfair Commercial Practices Directive – Particularly Articles 6 prohibits misleading and unfair commercial behaviour that causes or is likely to cause consumer(s) to take a transactional decision that would not have been taken otherwise, AI Act - Article 5 restricts certain manipulative uses of AI systems.	
--	---	--