DIGITAL OMNIBUS AND OMNIBUS ON AI

Position Paper VNO-NCW and MKB-Nederland

9 February 2026

VNO-NCW and MKB-Nederland welcome the simplification efforts of the European Commission to make the vast and complex digital & data rules more harmonized, predictable, proportionate, coherent and easier to implement. This reduces the burden on companies, increases responsible (innovative) development and adoption of AI without lowering the objectives of the Rulebook.

The Digital omnibus and the Omnibus on AI presented by the European Commission on 19th November, are a good first step towards this and we hope more will follow[1]. Although we support many of the efforts, we also have some concerns, specifically regarding the proposal for a Single entry Point for cyber- and privacy incidents.

Summary

Omnibus on AI

We support the proposals set out in the Omnibus on AI where they strengthen legal certainty and make compliance more workable. This includes the proposal to postpone deadlines for high-risk AI obligations to allow time for the development of standards and clearer guidance on the AI Act and its interaction with other EU rules. However, we are concerned about the possibility for the Commission to decide on an earlier deadline once the standards and guidance are published. We would prefer a fixed and realistic deadline to avoid legal uncertainty about the date of application, focus on high quality clarification and ensure that notified bodies[2] can be formally notified on time to perform the

[1] We refer to the position papers of BusinessEurope with many examples of inconsistencies, unclarities and overlaps[1] which need addressing: Reducing regulatory burden to restore the EU's competitive edge - BusinessEurope (December 2025); Simplifying the EU digital rulebook - a BusinessEurope position paper - BusinessEurope (July 2025)

[2] With regard to annex I high risk AI systems

required third party conformity assessments.[3]
We also support the proposal allowing (under strict safeguards) exceptional processing of special categories of personal data for bias detection & mitigation to prevent discrimination beyond high-risk AI. In addition, we back the proposals to oblige the Commission and Member States to promote AI literacy and skills (not limited to the working force), to remove disproportionate EU database registration for low-risk AI systems that fall within the broad scope of Annex III but are not high-risk applications, to extend simplified quality management system approaches from micro-enterprises to SMEs and improving cooperation among competent authorities. We also support the extension of real-world testing to high-risk AI systems embedded in products.

Digital Omnibus
We also support key proposals in the Digital Omnibus aimed at clarifying and better aligning GDPR with the wider digital framework. This includes proposals for targeted GDPR amendments to improve consistency, to clarify the demarcation between pseudonymised and personal data, and to explicitly confirm that "scientific research" covers academic, industrial and SME R&D, subject to the strict safeguards in the GDPR[4]. We support proposals to address the handling of special-category data in AI datasets, including clarification that residual traces may remain where removal is disproportionate after appropriate preventive measures have been taken, coupled with an obligation to apply effective measures to prevent disclosure or reappearance in outputs. We also support the proposal to confirm that legitimate interest can serve as a legal basis for developing and operating AI, subject to the usual balancing test and full compliance with GDPR principles and obligations. However, for legal certainty and level playing field purposes, we call for improving the clarity of aforementioned proposals.

Also, we welcome the Digital Omnibus proposals for burden reduction: including a more proportionate approach of access rights (in the event of misuse of rights), exception to information duties where individuals already have the information, and more proportionate breach notification requirements (e.g., notifying authorities only of high-risk breaches, using a harmonised template, and applying a more realistic 96-hour deadline). However, we call for improving the clarity of the proposals to ensure legal certainty. In the context of burden reduction, we also support the proposals for harmonised DPIA lists, templates and methodologies; further consolidation of data rules in the Data Act; and – for the enablement of data spaces - a more proportionate regime for data intermediation services through functional (rather than legal) separation and reduced obligations. In addition, we support stronger trade secret protections to

[3] Such notification process takes around a year.
[4] Article 89 GDPR

refuse data sharing where third-country jurisdiction risks are high. We further support proposals to limit B2G data sharing obligations to public emergencies, and to introduce a lighter cloud switching regime for customised services (concluded before 12 september 2025).

At the same time, we have concerns about specific proposals and how they could be designed or implemented. On biometrics (1-to-1 verification), we are concerned about approaches that create a new exception under Article 9 GDPR; we would instead favor a clarification that 1-to-1 verification falls outside Article 9. On cookies and ePrivacy, we are cautious that proposals promoting automated or machine-readable preference mechanisms. These mechanisms could reduce direct interaction between businesses and users, with potential negative effects—particularly for smaller firms.

We have concerns about the proposal to create a single central EU Single Entry Point platform for incident reporting across cyber and privacy. While intended to streamline reporting, it would increase security and national-security risks by creating a high-value central target. We would instead support a proposal based on one national reporting hub per Member State, with interoperable easy onward transmission – where required - to the relevant competent authorities.

In the following paragraphs we will explain our position in more detail.

I. Our assessment of the Digital Omnibus on AI proposal

AI ACT: Postponement of implementation deadlines high-risk AI

VNO-NCW and MKB-Nederland underwrite the importance of needing to improve implementation periods of new rules. Clarity on how to comply as well as reasonable periods to implement new obligations, is imperative to ensure that rules can be effectively implemented and supported.

Applying a pressure cooker both on the drafting of new laws as well as on the implementation thereof, does not help to meet the intended objectives and only puts an unnecessary burden on businesses working hard to comply with the new rules (in interaction with the existing rules). Let's not kid ourselves, making sense of the complex rules – and interaction with other rules – is not an easy task.

The proposal of the European Commission to postpone the implementation deadlines for high-risk AI systems[5] is welcome as clarity on how to comply as well

[5] The entry into application on Article 6(2) and Annex III is postponed maximum until 2 December 2027; and for Article 6(1) and Annex I maximum until 2 August 2028.

as interplay with existing rules, is still lacking, not in the least for SMEs. Realistic implementation deadlines are a prerequisite for correct and timely compliance.

However, the condition triggering applicability on an earlier date if meaningful clarity is provided beforehand (standards, guidance and compliance support tools are ready), contributes to legal uncertainty. We agree that undue delay should be minimized but it is more important to ensure high quality results (standards, guidance and tools) and making sure companies, specifically SMEs, have sufficient time to take stock of the standards, guidelines and tools in order to adequately implement the rules. It would be preferred if the date of application is postponed by a fixed period to provide for the necessary predictability.

AI ACT: Broader legal ground for bias detection and mitigation

The European Commission proposes to broaden the legal ground for processing special categories of personal data for bias detection and mitigation. This broadening of the scope to also detect and mitigate bias in non-high risk AI enables the detection, prevention and mitigation of bias in all AI systems takes into account the existing safeguards and strict conditions included in the AI Act for high-risk AI. See hereunder under the heading 'existing safeguards'. VNO-NCW and MKB-Nederland support the European Commission in its reasoning that bias detection, prevention and correction constitutes a substantial public interest, to protect natural persons from biases' adverse effects, including discrimination.

Although the detection and mitigation of bias is most important in high-risk AI systems, it is good to note that discrimination and other forms of harmful bias is not limited per se to high-risk AI systems. VNO-NCW and MKB-Nederland support that providers and deployers of non-high risk AI *may exceptionally* process specific categories of personal data to detect and mitigate bias if this is necessary to protect natural persons from biases' adverse effects, including discrimination.

Existing safeguards

The AI Act already includes a legal ground[6] for the processing of special categories of personal data for bias detection and mitigation *for high-risk AI*. This legal ground can only be used exceptionally and subject to appropriate safeguards and is subject to 6 explicit conditions: (a) other data - including synthetic data - is insufficient to detect and mitigate bias; (b) technical limitations on re-use and state-of-the-art security and privacy preserving measures (including pseudonymization) are in place; (c) secure access: including strict controls and documentation of access to the data, avoidance of misuse and only

[6] Article 9 paragraph 2 sub g GDPR jo article 10 paragraph 5 AI Act

accessible to authorized persons under the obligation of confidentiality; (d) the specific categories of personal data may not be transmitted, transferred or otherwise accessed by other parties (e) the specific categories of personal data must be deleted after purpose of bias detection or mitigating is met; and (f) the strict necessity of processing of the specific categories of personal data needs to be explicitly recorded.
The existing legal ground to process special categories of data is included to enable providers and deployers to meet the obligation of the AI Act (article 10.2) to detect, prevent and mitigate bias that is likely to affect health and safety of persons, have a negative impact on fundamental rights or lead to prohibited discrimination mitigation in training, validation and testing data sets.

AI ACT: AI Literacy

We support the European Commission tasking itself and the Member States to foster AI literacy instead of burdening all companies, large and small, with a disproportionate broad obligation which not seems to be limited to the provision or deployment of high-risk AI. We have been asking our government to include Digital (AI) literacy in the curriculum in the Netherlands for years. We agree with the European Commission that AI literacy should be a strategic priority. AI literacy should not only focus on the work force but on the whole of society. It is therefore important, that the Member States together with the European Commission in a coordinated manner, are tasked with ensuring a sufficient level of AI literacy of all EU citizens. It is important to ensure synergy between MMs and between the Commission and the MMs to prevent fragmentation in the EU.

It is also good to note that article 4 is not the only AI literacy obligation in the AI Act. The important **other** obligation of the AI Act is for providers and deployers to ensure AI literacy of their humans-in-the-loop.[7] Providers and deployers are required to ensure that persons tasked as human-in-the-loop have the necessary competence, training, authority and necessary support needed to fulfil this task. We underwrite this obligation of the AI Act. However, more guidance is required for companies to fulfil this important task.

AI ACT: Reducing the registration burden

VNO-NCW and MKB-Nederland support the proposal of the European Commission to delete the disproportionate obligation for providers to register AI systems in the EU database under Annex III, in the event their AI systems are not considered a high-risk application of AI. We have advocated for the exemption in article 6(3) AI Act because the Annex III high-risk areas are very broadly defined. It is important that the vast obligations for high-risk AI applications are indeed limited to high-risk AI applications and do not include non-high-risk applications

[7] Article 26(2) AI Act

in their slipstream. Such as AI applications which are only used for preparatory tasks and where a human does not base its decision solely on this input. For instance, a HR assessment which uses a AI module to determine a person's level of AI literacy. This would fall within the scope of one of the high-risk areas of Annex III (4a). But if the whole selection-assessment includes, besides that one AI component, many face-to-face elements, such as face-to-face discussions, face-to-face interviews, in-person games etc. It would be disproportionate to classify the whole assessment as high-risk AI due to that one AI component.

If we follow the logic of the DPAs, registering of low-risk preparatory AI components need to be registered for them to be able to check whether the assessment has been done right. But do we seriously need a registration of all those non-high risk AI applications, just in case DPAs have the resources and time left to check this? Or do we want the DPAs to focus on truly high-risk applications? Chances are that the majority if not all those registrations will not be used at all by the DPAs. In the context of burden reduction at least such 'just in case' registration requirements for low risk applications of AI need to be deleted.

AI ACT: Extending derogations of micro-enterprises to SMEs

VNO-NCW and MKB-Nederland support the proposal of the European Commission to extend the derogation from micro-enterprises to SMEs to comply with certain elements of the quality management system in a simplified manner. Harmonized and simplified formats, easy to use harmonized online implementation tools as well as proportionality and a risk-based approach are important burden reduction measures for SMEs.

AI ACT: Cooperation competent authorities

VNO-NCW and MKB-Nederland support proposals to strengthen the cooperation between competent authorities to provide each other with mutual assistance necessary for fulfilling their respective mandates, with a view to ensuring coherent application of this Regulation and Union law. It is important that the competent authorities take each other's point of view into account as well as the practical implications for companies of implementing all the complex and interplaying rules.

II. Our assessment of the Digital Omnibus proposal (Data, GDPR and cyber reporting)

Targeted amendments to the GDPR

VNO-NCW and MKB-Nederland welcome targeted amendments to the GDPR which increase the clarity of the provisions, improve the coherence with other

rules of the Digital rulebook, make the rules more predictable, proportionate, risk-based and easier to implement. This will improve the aim of that GDPR, which is to ensure a balance between the free movement of personal data and the protection of privacy.

VNO-NCW and MKB-Nederland encourage the development and adoption of trustworthy AI which is key in providing for economic growth and supporting innovation with socially beneficial outcomes.

GDPR: Definition personal data

VNO-NCW and MKB-NL welcome the effort to clarify that the existence of additional data that could be used to identify the data subject does not in itself imply that pseudonymized data must be considered personal data in all cases and for everyone (to align with the ECJ SRB case). It depends on the means reasonably likely to be used to identify the natural person by the actual recipient(s)[8].

The proposal of the European Commission confirms that pseudonymization, depending on the circumstances of the case, can effectively prevent persons other than the controller from identifying the data subject in such a way that the data subject is not or no longer identifiable to them.[9]

The proposal does not lower the existing threshold of 'not having the means'. The recipient is still only considered 'not to have the means' when identification of the data subject is prohibited by law or is impracticable in practice, for example because it requires an excessive effort in terms of the time, costs, and manpower required, so that the risk of identification appears negligible in reality.[10]

But this proposal has received many reactions, making it clear that the wording of the proposed Article 4 is not clear for everyone. Because clarity is an essential requirement of legal certainty, we suggest to improve the wording to better reflect the meaning of the SRB ruling and to prevent misinterpretation of this key definition.

Specifically smaller controllers need more support with respect to the criteria and means to determine whether data resulting from pseudonymization does not constitute personal data for another person.

---

[8] See recital 80 of the ECJ EDPS/SRB ruling: "As the Advocate General observed, in essence, in point 51 of his Opinion, those clarifications relating to the assessment of whether or not the data subject is identifiable would be deprived of any practical effect if pseudonymised data were to be regarded as constituting, in all cases and for every person, personal data for the purposes of the application of Regulation 2018/1725."; see also recital 82 of the ECJ SRB ruling.

[9] See recital 87 ECJ SRB ruling

[10] See recital 46 Breyer ECJ ruling

GDPR: Definition scientific research

VNO-NCW and MKB-Nederland also welcome the effort to clarify the definition of *scientific research.* The proposal explicitly confirms that scientific research includes research and technology development (innovation) in academic, industry and other settings such as SMEs. This is the interpretation of scientific research as was initially foreseen by the legislators. The clarification does not alter the requirements for scientific research: research needs to be of high quality and meet the conditions of scientific research, such as methodological and systematic approach. The clarification proposal further clarifies that further processing *for scientific purposes* is compatible with the initial purpose of processing. This clarification is needed because, although it was originally intended to be interpreted as aforementioned, it has not always been interpreted accordingly. It also explicitly clarifies that scientific research constitutes a legitimate interest.[11] This is a codification of the ECJ KNLTB ruling[12] in which the European Court of Justice confirmed that all *lawful* interests can in principle be legitimate interests. This is a welcome codification to ensure harmonized interpretation and enforcement across Member States. The GDPR balances the right to protection of personal data, pursuant to Article 8 CFREU, with the freedom of science, pursuant to Article 13 CFREU[13]. The conditions and safeguards of article 89 GDPR remain unchanged. The proposal provides clarity but does not lower the intended protection and purpose of the GDPR, the principles and obligations of the GDPR still need to be taken into account. This is a welcome clarification to ensure harmonized interpretation and enforcement across Member States.

GDPR: Residual traces special categories data

VNO-NCW and MKB-Nederland welcome the clarification in Article 9 regarding the *residual* processing of special categories of personal data in AI training, testing or validation data sets where removal of such data requires *disproportionate* effort. This exemption does not undermine the obligation of the provider of an AI system or model to mitigate risks through appropriate technical and operational measures with regard to the collection and otherwise processing of special categories of personal data. If despite aforementioned measures been taken, residual traces of special categories of personal data appear and the removal of those residual traces requires disproportionate effort, the provider is obligated to undertake effectively technical and operational measures to

[11] Article 6(1)(f) GDPR.
[12] ECJ ruling KNLTB vs AP; 4 October 2024, Case C-621/22
[13] See recital 32 GDPR.

mitigate the risk of those residual traces of special categories of data from further appearing in outputs or otherwise being disclosed. The principles and obligations of the GDPR still need to be taken into account. This proposal provides clarity and is aligned with the aim of the GDPR to ensure a balance between the free movement of personal data and the protection of privacy. Also, it is important to make a distinction between special categories of personal data relating to a public figure and non-public figures. Special categories of personal data and criminal data about public persons may be legitimately included on the basis of article 9.2.g jo article 11 ECHR (freedom of information). For instance, religious beliefs of the pope and political opinions of parliament members.[14]

GDPR: Biometric verification

The proposal to include an exemption in article 9 regarding the processing of biometric data for the mere verification of a natural person (one-on-one) raises some questions. The acknowledgement is welcome that the temporary processing of biometric data for the mere confirmation of an individual already known to the controller, is a low risk processing activity. However, in our opinion, an exemption is not needed. History of the GDPR shows that the processing of biometric data for mere verification purposes was not intended to fall within the scope of article 9 GDPR. Therefore, a mere clarification that one-on-one verification falls outside the scope of the ban of article 9 GDPR is sufficient.

In addition, VNO-NCW and MKB-Nederland questions the inserted condition that the biometric data or the means needed for the verification need to be under the sole control of the data subject. Which means that the data subject holds the biometric template or the decryption key to access the template. To ensure that the controller does not gain knowledge of the biometric data, or only for the limited time of the verification process. This is included to prevent further processing of the biometric data (without the active involvement of the data subject). We question whether the requirement - that the data subject holds the biometric template or the decryption key to access the template – is aligned with common secure and accepted practices, such as in high security facilitations. For instance, if verification is needed to gain strict secure access (e.g. nuclear power plant), we question whether it is feasible that the data subject holds the biometric template or the decryption key to access the template.

Instead of an exemption, we would welcome the acknowledgement that verification falls outside the scope of article 9 GDPR. This would also align with the risk based approach of the GDPR, align with the AI Act and be a welcome clarification to ensure harmonized interpretation and enforcement across Member States.

[14] See Case C-507/17, Google LLC vs CNIL et al, 24 September 2019, para 60

GDPR: Legitimate interest – AI

VNO-NCW and MKB-Nederland welcome the explicit clarification that legitimate interest can be a legal ground for processing personal data in the context of the development and operation of an AI system, except where other Union or national laws explicitly require consent. This proposal provides clarity but does not lower the intended protection and purpose of the GDPR. The proposal merely makes explicit that legitimate interest can be a used as a legal ground for processing of personal data within the context of the development and operation of AI systems *provided* the legitimate interest of the controller or a third party meets the required 3-step test. Meaning that the interest must be legal and the processing is strictly necessary for the purposes of the legitimate interest in question and that, in the light of all the relevant circumstances, the interests or fundamental rights and freedoms of the data subjects do not override that legitimate interest of the controller (or relevant 3rd party). The other principles and obligations of the GDPR also still need to be taken into account, such as data minimalization, purpose limitation etc. This proposal is a codification of the ECJ KNLTB ruling[15] in which the European Court of Justice confirmed that all *lawful* interests can in principle be legitimate interests. This is a welcome codification to ensure harmonized interpretation and enforcement across Member States. This reassurance is important to build a strong position on trustworthy AI which is key in providing for economic growth and supporting innovation with socially beneficial outcomes. However, VNO-NCW/MKB-NL is concerned about the unconditional right to object[16], which could require halting AI training on a data subject's personal data. This is technically impossible for existing models or inferred data, and retroactive removal would necessitate retraining, which is practically very challenging. VNO-NCW/MKB-NL therefore proposes to clarify that the right to object only applies prospectively.

GDPR: Risk based approach

VNO-NCW and MKB-Nederland welcome the necessary clarification that low-risk processing of personal data requires a less intensive approach than high-risk processing of personal data. This principle of proportionality is made more explicit in the Digital Omnibus proposal regarding the right of access, information requirements and data breach notifications.

[15] ECJ ruling KNLTB vs AP; 4 October 2024, Case C-621/22
[16] Art. 88c as proposed in the Digital Omnibus

GDPR: Abuse of the right of access

VNO-NCW and MKB-Nederland welcome the acknowledgement that in practice the right of access is not always used by data subjects to be granted access to their personal data but instead to be paid a compensation, potentially even under the threat of bringing a claim for damages or offer to withdraw the request in return for compensation. Or situations where data subjects make excessive use of the right of access with the only intent of causing damage or harm to the controller, in particular because of their repetitive character. Such requests place a significant burden on companies, specifically SMEs. It is important that companies can focus their efforts on legitimate access requests.

Within this context, VNO-NCW and MKB-Nederland welcome keeping the burden of proof to a reasonable extent regarding the excessive character of a request. However, specifically SMEs need more guidance (including examples) about what concretely constitutes an 'excessive request'.

GDPR: Information requirements

VNO-NCW and MKB-Nederland support the proposal that information about the processing of personal data does not have to be provided if there are reasonable grounds to expect the data subjects already has that information. For instance, if you rent a car you can expect the rental company to process information about who you are (name and address) and if you have a drivers' license (and for which type of vehicles). For this exemption to kick in, the processing needs to be non-intensive (not complex and low amount of personal data), not likely to result in a high-risk (within the meaning of article 35) and a direct relationship exists between controller and data subject (such as baker, hairdresser, car rental, carpenter, shoemaker or other small retailer, craftsman or local sports club). This exemption benefits small operators, it reduces the disproportionate burden on such small operators in low-risk situations where the processing of personal data is not the core activity of the controller.

VNO-NCW and MKB-Nederland have concerns about the condition that the controller may not transmits the data to other recipients or categories of recipients. A small company or club may under normal circumstances not transmit the data to other recipients but it will always need to comply with legal orders by competent authorities, including the police or a district attorney. VNO-NCW and MKB-Nederland would welcome further clarification that legal orders fall outside the scope of aforementioned condition.

VNO-NCW and MKB-Nederland also welcome the exemption to the information requirement with regard to scientific research. Specifically for the situation where the controller at the time of collection of the personal data did not know that it would process personal data for scientific research purposes at a later stage. The controller may inform data subjects by making the information publicly available in a manner that as many data subjects concerned are reached.

GDPR: Data breach notifications

VNO-NCW and MKB-Nederland welcome the proposal to introduce a higher threshold for data breach notifications to the *competent authority*. It is good to note that the threshold for notification to the data subject remains the same. The proposal requires notifications to the competent authority (Data Protection Authority) only to be submitted if a data breach is likely to result in a high risk to the rights and freedoms of the data subject. This coincides with the instances where a data subject needs to be notified by the controller. This proportionate approach reduces disproportionate notification burdens and enables companies and competent authorities to focus their efforts on data breaches which are likely to result in a high-risk. VNO-NCW and MKB-Nederland also welcome the proposal for a harmonized common template for notifying data breaches, a common (dynamic and non-exhaustive) list of circumstances in which a personal data breach is likely to result in a high risk, as well as the proposal to extend the deadline for data breach notification from 72 to 96 hours. These proposals are specifically helpful for SMEs (they can focus their limited resources on high-risk situations), although they are still required to document all low risk data breaches and the mitigating measures they have undertaken (in case a DPA asks for this).

GDPR: Data Protection Impact Assessment (DPIA)

VNO-NCW and MKB-Nederland welcome a harmonized list of processing activities that require a DPIA, a harmonized list of common processing activities which do not require a DPIA as well as a harmonized template and methodology for conducting a DPIA and subsequent reporting. This would bring necessary clarification and harmonization about an obligation which requires a lot of resources, specifically of SMEs.

e-Privacy Directive & GDPR: Cookies and similar techniques

VNO-NCW and MKB-Nederland have been asking for a solution for the consent fatigue for a long time. The interplay between the e-Privacy directive[17] and the

[17] Article 5(3) of the ePrivacy directive, 2002/58/EC on privacy and electronic communications

GDPR increases the complexity for companies.

The ePrivacy Directive applies to the placement of cookies or similar technologies to gain information from a user's terminal equipment, while the subsequent processing of personal data is subject to the GDPR. Under the ePrivacy Directive consent is the required legal basis for cookies but the legal processing grounds for the subsequent processing can be one of the 5 other legal grounds of the GDPR. For instance, necessity for the performance of a contract.

The complexity of the interplay between these 2 pieces of legislation has led to legal uncertainty and subsequent higher compliance costs. In addition, in some Member States, such as in the Netherlands, two different national authorities are tasked with the supervision of the different rules and two different ministries are responsible for the different legal frameworks.

VNO-NCW/MKB-Nederland welcome the efforts to simplify the interplay of the rules on cookies (and similar technologies) and possible subsequent processing of personal data. We support the proposal that processing of personal data on and from terminal equipment will be governed only by the GDPR. We also support that the ePrivacy Directive will be remain applicable for connected devices of legal persons and the use of cookies (and similar techniques) pertaining to non-personal data if and in so far necessary to protect the confidentiality of communication on public electronic communication networks.

However, we have concerns about consent as the sole legal processing ground for accessing terminal equipment of a natural person when personal data is collected.

Notwithstanding that the proposed amendments provide for certain exemptions where it should not be necessary to obtain consent and where the subsequent processing should be considered lawful, in particular where they pose a low risk to the rights and freedoms of the data subjects or where the placement of such technologies is necessary for the provision of a service requested by the data subject, this does not provide for other instances where consent is also not the proper legal processing ground. For instance, consent is not the proper legal processing ground with regard to the employee-employer relationship if the processing activity is not solely beneficial for the employee. For example, an employer needs to be able to control its internal communication systems, including terminal equipment, in the event of grounded suspicion of fraud or corporate espionage. It is therefore necessary to be able to apply the most appropriate legal processing ground depending on the purpose of a given processing activity.

In addition, VNO-NCW and MKB-Nederland has concerns about the proposal paving the way for automated and machine-readable indications of individual choices. This, again, does not take into account that consent is not the only proper legal processing ground; and the possibility of making automated choices is not per se granular. Being able to efficiently and effectively advertise for products and services is an important marketing tool for all companies, big and small. VNO-NCW and MKB-Nederland stress the importance of the possibility for individuals to choose from which specific (trusted) company they would (or not) like to receive (tailored and contextual) advertisements. The proposal seems to support the possibility of granular choices where they refer to agentic AI as support tool for persons in making specific consent choices. But, the possibility of granular choices needs to be the default proposition where consent is the proper legal processing ground, to allow for direct interaction between companies and its (prospective) customers. . To truly battle consent fatigue, it is important to allow for all 6 legal processing grounds of the GDPR. It is also important to take into consideration that there is no strict hierarchy between the six legal grounds for processing personal data.[18]

In addition, VNO-NCW/MKB-Nederland is concerned about the requirement that a company may not ask for consent again within a time period of 6 months. This is a long period and would entail the storage of personal data (the refusal) for at least six months.

NIS, CER, CRA and GDPR: Single Entry Point (Cybersecurity and Data Breach incidents)

VNO-NCW and MKB-Nederland are not in favor of a single central reporting platform at the European level. VNO-NCW and MKB-Nederland would support a single reporting platform at the national level.

For the majority of companies based in the Netherlands and covered by NIS2 or CER there is little or no efficiency gain in a SEP on European level. More importantly, VNO-NCW and MKB-Nederland has concerns about the security of a European central platform and database. This might prove an attractive target for criminals, state actors, etc. In short, a risk to national security.

VNO-NCW and MKB-Nederland supports a single reporting platform at Member state (national) level. The EC or ENISA could possibly provide/draw up guidelines for this. In the Netherlands, the necessary steps are being taken to set up a single reporting platform at national level: reports from NIS2, CER, CRA, and Netcode will soon all be able to be reported to the National Cyber Security Center (NCSC). The NCSC will subsequently forward them to the supervisory

[18] See Opinion of Advocate General Szpunar in Case C-394/23, Mousse (ECLI:EU:C:2024:610), para 28

authorities. VNO-NCW and MKB-Nederland support using the same point for reporting Data breaches under the GDPR.

Data access and sharing

Consolidation data rules

VNO-NCW and MKB-Nederland support the efforts to consolidate the EU data rules[19] in the Data Act. Coherence between the different rules of the digital rulebook is a prerequisite for clarity and subsequent legal certainty. However, further proposals would be welcome to ensure coherence between aforementioned data rules and the GDPR.

VNO-NCW and MKB-Nederland support the proposals to facilitate the economic viability and growth of data intermediation services providers. To this end, we concur that the obligation to keep data intermediation services legally separate from any other service a company may want to offer, is a problematic obligation in terms of economic viability. VNO-NCW and MKB-Nederland support the proposal to replace this troublesome obligation with the obligation to solely keep the different services functionally separate. VNO-NCW and MKB-Nederland also support the proposal to drastically shorten the list of obligations.

Data Act: Trade secrets

VNO-NCW and MKB-Nederland support the proposal to further strengthen the trade secrets protection in the Data Act. In the context of improving our resilience, the proposal to include the possibility for data holders to refuse data sharing requests if this poses a high risk of unlawful acquisition, use, or disclosure to third country entities that are subject to jurisdictions with weaker protections than those available in the Union. However, for companies it might not always be possible to provide the necessary proof of such high-risk, specifically for smaller companies. It should therefore not be required of individual companies to undertake a costly assessment of international law and practices. Refusing a data sharing request should be possible on the basis of general knowledge. VNO-NCW and MKB-Nederland also request the inclusion of an obligation for the European Commission and Member States to provide general assistance (e.g. adequacy decisions). It is not realistic to require SMEs to conduct extensive third-country-law analyses.

Data Act: B2G data sharing

VNO-NCW and MKB-Nederland support the proposal to narrow the scope of

[19] Free Flow of Non-personal Data Regulation, Data Governance Act, the Open Data Directive and Data Act.

chapter 5 (B2G data sharing) of the Data Act to public emergencies (instead of exceptional needs). Governments can request data from companies when necessary to respond to a public emergency or to mitigate or support the recovery from a public emergency

Data Act: Cloud switching

VNO-NCW and MKB-Nederland support the proposed lighter regime for switching between cloud service providers when custom made cloud service are provided and the contract is concluded before 12-9-25 and the term custom build is not too broadly interpreted. Custom made cloud services are data processing services that are not off-the-shelf and would not function without prior adaptation to the specific needs and system of the user. VNO-NCW and MKB-Nederland also support the exemption for SMEs (and SMCs) cloud service providers when the contract was concluded before 12-9-25; as well as the clarification that these providers can include early-termination penalties in fixed-term contracts.

Irvette Tempelman
VNO-NCW/MKB-Nederland
tempelman@vnoncw-mkb.nl

Bijlage 1 -

Guidance under preparation by the Commission include:

• Guidelines on the practical application of the high-risk classification;
• Guidelines on the practical application of the transparency requirements under Article 50 AI Act;
• Guidance on the reporting of serious incidents by providers of high-risk AI systems;
• Guidelines on the practical application of the high-risk requirements;
Guidelines on the practical application of the obligations for providers and deployers of high-risk AI systems;
• Guidelines with a template for the fundamental rights impact assessment;
• Guidelines on the practical application of rules for responsibilities along the AI value chain;
• Guidelines on the practical application of the provisions related to substantial modification;
• Guidelines on the post-market monitoring of high-risk AI systems;
• Gudelines on the elements of the quality management system which SMEs and SMCs may comply with in a simplified manner;
• Guidelines on the AI Act's interplay with other Union legislation, for example joint guidelines of the Commission and European Data Protection Board on the interplay of the AI Act and EU data protection law, guidelines on the interplay between the AI Act and the Cyber Resilience Act, and guidelines on the interplay between the AI Act and the Machinery Regulation;
• Guidelines on the competences and designation procedure for conformity assessment bodies to be designated under the AI Act.

Irvette Tempelman
VNO-NCW/MKB-Nederland
tempelman@vnoncw-mkb.nl