Council of the European Union
General Secretariat

Interinstitutional files:
2025/0360 (COD)

Brussels, 06 February 2026

WK 1701/2026 ADD 2

LIMITE

SIMPL
ANTICI
DATAPROTECT
CYBER
TELECOM
CODEC
PROCIV
COMPET
MI

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From:	General Secretariat of the Council
To:	Antici Group (Simplification)
Subject:	Additional Comments from MS on Omnibus VII (Digital Omnibus) - GDPR and P2B – written Consultation (DDL on 30/01/2026)

Following the written consultation on Omnibus VII (Digital Omnibus) – GDPR and P2B, delegations will find Additional comments received from CZ.

Guidelines to be followed

Please kindly provide your contributions in the table below.

Drafting suggestions: you may use '**track changes**'* or formatting (for example **bold-underline** for additions and ~~strike-through~~ for deletions, **where necessary, in a different colour**). *Track changes can only be connected once the cursor is placed in editable areas (Drafting or Comments columns).

To make it feasible to consolidate all contributions, the structure of the table must not be changed, so **no rows can be added or deleted.**

New provisions may only be added in any of the **'existing cells'.**

Name of document: please add the **two initials** of your delegation's country followed by a space (to the MS Word document name), followed by any optional text, for example, for Austria: **AT comments on … .docx**

Thank you for your cooperation!

Commission proposal	Drafting suggestions	Comments
General Comments		
Proposal for a		
REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL		
amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU)		

Commission proposal	Drafting suggestions	Comments
2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus)		
THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,		
Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 and 114 thereof,		
Having regard to the proposal from the European Commission,		
After transmission of the draft legislative act to the national parliaments,		
Having regard to the opinion of the European Economic and Social Committee[1],		

1 OJ C […], […], p. […].

Commission proposal	Drafting suggestions	Comments
Having regard to the opinion of the European Central Bank[2], 2 OJ C […], […], p. […].		
Having regard to the opinion of the Committee of the Regions[3], 3 OJ C […], […], p. […].		
Acting in accordance with the ordinary legislative procedure,		
Whereas:		
[…]		
(27) This Regulation proposes a series of targeted amendments to Regulation (EU) 2016/679 for clarification and simplification, whilst preserving the same level of data protection. Article 4 of Regulation (EU) 2016/679 provides that personal data is any information relating to an	~~(27) This Regulation proposes a series of targeted amendments to Regulation (EU) 2016/679 for clarification and simplification, whilst preserving the same level of data protection. Article 4 of Regulation (EU) 2016/679 provides that personal data is any information relating to an~~	CZ: The recital relates to the proposed definition of personal data. CZ preferes other more suitable means of more precise definition of identifiability, which would not unproportionately decrease legal certainity.

Commission proposal	Drafting suggestions	Comments
identified or identifiable natural person. In order to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used to identify the natural person directly or indirectly. Taking into account the case-law of the Court of Justice of the European Union concerning the definition of personal data, it is necessary to provide further clarity on when a natural person should be considered to be identifiable. The existence of additional information enabling the data subject to be identified does not, in itself, mean that pseudonymised data must be regarded as constituting, in all cases and for every person or entity, personal data for the purposes of the application of Regulation (EU) 2016/679. In particular, it should be clarified that information is not to be considered personal data for a given entity where that entity does not have means reasonably likely to be used to identify the natural person to whom the information relates. A potential subsequent transmission of that information to third parties who have means reasonably allowing them to identify the natural person to whom the information relates, such as cross-checking with other data at their disposal, renders that information personal data only for those third parties who have such means at their disposal. An entity for which the information is not personal data, in principle, does not fall within the scope of application of Regulation (EU) 2016/679. In this respect the Court of Justice of the European Union	~~identified or identifiable natural person. In order to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used to identify the natural person directly or indirectly. Taking into account the case-law of the Court of Justice of the European Union concerning the definition of personal data, it is necessary to provide further clarity on when a natural person should be considered to be identifiable. The existence of additional information enabling the data subject to be identified does not, in itself, mean that pseudonymised data must be regarded as constituting, in all cases and for every person or entity, personal data for the purposes of the application of Regulation (EU) 2016/679. In particular, it should be clarified that information is not to be considered personal data for a given entity where that entity does not have means reasonably likely to be used to identify the natural person to whom the information relates. A potential subsequent transmission of that information to third parties who have means reasonably allowing them to identify the natural person to whom the information relates, such as cross-checking with other data at their disposal, renders that information personal data only for those third parties who have such means at their disposal. An entity for which the information is not personal data, in principle, does not fall within the scope of application of Regulation (EU) 2016/679. In this respect the Court of Justice of the European Union~~	

Commission proposal	Drafting suggestions	Comments
has held that a means of identifying the data subject is not reasonably likely to be used where the risk of identification appears in reality to be insignificant, in that the identification of that data subject is prohibited by law or impossible in practice, for example because it would involve a disproportionate effort in terms of time, cost and labour. An example of a prohibition against reidentification can be found in the obligations of health data users in Article 61(3) of Regulation (EU) 2025/327 of the European Parliament and of the Council[4]. The Commission, together with the European Data Protection Board, should support controllers in the application of this updated definition by stipulating technical criteria in an implementing act. 4 Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 (OJ L, 2025/327, 5.3.2025, ELI: http://data.europa.eu/eli/reg/2025/327/oj)	~~has held that a means of identifying the data subject is not reasonably likely to be used where the risk of identification appears in reality to be insignificant, in that the identification of that data subject is prohibited by law or impossible in practice, for example because it would involve a disproportionate effort in terms of time, cost and labour. An example of a prohibition against reidentification can be found in the obligations of health data users in Article 61(3) of Regulation (EU) 2025/327 of the European Parliament and of the Council[4]. The Commission, together with the European Data Protection Board, should support controllers in the application of this updated definition by stipulating technical criteria in an implementing act.~~ ~~4 Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 (OJ L, 2025/327, 5.3.2025, ELI: http://data.europa.eu/eli/reg/2025/327/oj)~~	
(28) In order to assess whether research meets the conditions of scientific research for the purpose of this Regulation, account can be taken of elements such as methodological and systematic approach applied while conducting the research in the specific area. Research and technology		

Commission proposal	Drafting suggestions	Comments
development should be conducted in academic, industry and other settings, including small and medium-sized undertakings, (Article 179(2) TFEU) and should be always of a of high quality and should adhere to the principles of principles of reliability, honesty, respect and accountability (verifiability).		
(29) It should be reiterated that further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations. In such cases it is not necessary to ascertain on the basis of Article 6(4) of this Regulation whether the purpose of the further processing is compatible with the purpose for which the personal data are initially collected.		
(30) Trustworthy AI is key in providing for economic growth and supporting innovation with socially beneficial outcomes. The development and use of AI systems and the underlying models such as large language models and generative video models rely on data, including personal data, in various phases in the AI lifecycle, such as the training, testing and validation phase and may in some instances be retained in the AI system or the AI model. The processing of personal data in this context may therefore be carried out for purposes		

Commission proposal	Drafting suggestions	Comments
of a legitimate interest within the meaning of Article 6 of Regulation (EU) 2016/679, where appropriate. This does not affect the obligation of the controller to ensure that the development or use (deployment) of AI in a specific context or for specific purposes complies with other Union or national law, or to ensure compliance where its use is explicitly prohibited by law. It also does not affect its obligation to ensure that all other conditions of Article 6(1)(f) of Regulation (EU) 2016/679 as well as all other requirements and principles of that Regulation are met.		
(31) When the controller, in the light of the risk-based approach which informs the scalability of the obligations under this Regulation, is balancing the legitimate interest pursued by the controller or a third party and the interests, rights and freedoms of the data subject, consideration should be given to whether the interest pursued by the controller is beneficial for the data subject and society at large, which may for instance be the case where the processing of personal data is necessary for detecting and removing bias, thereby protecting data subjects from discrimination, or where the processing of personal data is aiming at ensuring accurate and safe outputs for a beneficial use, such as to improve accessibility to certain services. Consideration should also, among others, be given to reasonable expectations of the data subject based on their relationship with the controller,		

Commission proposal	Drafting suggestions	Comments
appropriate safeguards to minimise the impact on data subjects' rights such as providing enhanced transparency to data subjects, providing an unconditional right to object to the processing of their personal data, respecting technical indications embedded in a service limiting the use of data for AI development by third parties, the use of other state of the art privacy preserving techniques for AI training and appropriate technical measures to effectively minimise risks resulting, for example, from regurgitation, data leakage and other intended or foreseeable actions.		
(32) The processing of personal data for scientific research purposes and the application of the GDPR's provisions on scientific research are conditional on the adoption of appropriate safeguards for the rights and freedoms of data subjects, pursuant to Article 89(1) GDPR. To that end, 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. The processing of personal data for the purpose of scientific research therefore pursues a legitimate interest within the meaning of Article 6(1)(f) of Regulation (EU) 2016/679, provided that such research is not contrary to Union or Member State law. This is without prejudice to the obligation of the controller to ensure that all other conditions of Article 6(1)(f) of Regulation (EU)		

Commission proposal	Drafting suggestions	Comments
2016/679 as well as all other requirements and principles of that Regulation are met.		
(33) The development of certain AI systems and AI models may involve the collection of large amounts of data, including personal data and special categories thereof. Special categories of personal data may residually exist in the training, testing or validation data sets or be retained in the AI system or the AI model, although the special categories of personal data are not necessary for the purpose of the processing. In order not to disproportionately hinder the development and operation of AI and taking into account the capabilities of the controller to identify and remove special categories of personal data, derogating from the prohibition on processing special categories of personal data under Article 9(2) of Regulation (EU) 2016/679 should be allowed. The derogation should only apply where the controller has implemented appropriate technical and organisational measures in an effective manner to avoid the processing of those data, takes the appropriate measures during the entire lifecycle of an AI system or AI model and, once it identifies such data, effectively remove them. If removal would require disproportionate effort, notably where the removal of special categories of data memorised in the AI system or AI model would require re-engineering the AI system or AI model, the controller should effectively protect such data		

Commission proposal	Drafting suggestions	Comments
from being used to infer outputs, being disclosed or otherwise made available to third parties. This derogation should not apply where the processing of special categories of personal data is necessary for the purpose of the processing. In this case, the controller should rely on the derogations pursuant to Article 9(2)(a) – (j) of Regulation (EU) 2016/679.		
(34) Biometric data, as defined in Article 4(14) of Regulation (EU) 2016/679, means processing of certain characteristics of a natural person through a specific technical means and which allows or confirms the unique identification of that person. The notion of biometric data includes two distinct functions, namely the identification of a natural person or the verification (also called authentication) of his or her claimed identity, both of which rely on different technical processes. The identification process is based on a 'one-to-many' search of the data subject's biometric data in a database, while the verification process is based on a 'one-to-one' comparison of biometric data provided by the data subject, who is thereby claiming his or her identity. Derogating from the prohibition to process biometric data under Article 9(1) of the Regulation should also be allowed where the verification of the claimed identity of the data subject is necessary for a purpose pursued by the controller, and suitable safeguards apply to enable the data subject to have sole control of the		

Commission proposal	Drafting suggestions	Comments
verification process. For example, where the biometric data are securely stored solely at the side of the data subject or are securely stored at the side of the controller in a state-of-the-art encrypted form and the encryption key or equivalent means is held solely by the data subject, that processing is not likely to create significant risks to his or her fundamental rights and freedoms. The controller does not gain knowledge of the biometric data or only for a very limited time during the verification process.		
(35) Article 15 of Regulation (EU) 2016/679 provides data subjects with the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed and, where that is the case, access to the personal data and certain additional information. The right of access should allow the data subject to be aware of, and to verify, the lawfulness of the processing and enable him or her to exercise his or her other rights under Regulation (EU) 2016/679. By contrast, it should be clarified in Article 12 of the Regulation that the right of access, which is from the outset favourable to data subjects, should not be abused in the sense that the data subjects abuse them for purposes other than the protection of their data. For example, such an abuse of the right of access would arise where the data subject intends to cause the controller to refuse an access request, in order to subsequently demand the		

Commission proposal	Drafting suggestions	Comments
payment of compensation, potentially under the threat of bringing a claim for damages. Other examples of abuse include situations where data subjects make excessive use of the right of access with the only intent of causing damage or harm to the controller or when an individual makes a request, but at the same time offers to withdraw it in return for some form of benefit from the controller. Moreover, in order to keep their burden to a reasonable extent, controllers should bear a lower burden of proof regarding the excessive character of a request than regarding the manifestly unfounded character of a request. The reason is that the manifestly unfounded character of a request depends on facts that lie principally within the controller's sphere of responsibility, whereas the excessive character of a request concerns the possibly abusive conduct of a data subject, which lies primarily outside the controller's sphere of influence, and therefore the controller may be able to prove such abuse only to a reasonable level. In any event, while requesting access under Article 15 of Regulation (EU) 2016/679 the data subject should be as specific as possible. Overly broad and undifferentiated requests should also be regarded as excessive.		
(36) Article 13 of Regulation (EU) 2016/679 requires the data controller to provide the data subject with certain information on the processing of his or her personal data as well as certain further		

Commission proposal	Drafting suggestions	Comments
information necessary to ensure fair and transparent processing, as defined in paragraphs 1, 2 and 3 of that provision. According to paragraph 4 of Article 13 of Regulation (EU) 2016/679, that obligation does not apply where and insofar as the data subject already has the information. To further reduce the burden of data controllers, without undermining the possibilities of the data subject to exercise his or her rights under Chapter III of the Regulation, this derogation should be extended to situations where the processing is not likely to result in a high risk, within the meaning of Article 35 of the Regulation, and there are reasonable grounds to assume that the data subject already has the information referred to in points (a) and (c) of paragraph 1 in the light of the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller. These should be the situations where the context of the relationship between the controller and the data subject is very clear and circumscribed and the controller's activity is not data-intensive, such as the relationship between a craftsman and their clients, where the scope of processing is limited to the minimum data necessary to perform the service. The controller's activity is not data-intensive where it collects a low amount of personal data and its processing operations are not complex, which is not the case, for example, in the field of employment. In such circumstances, that is to say when the processing is non data-intensive, non-complex and where the		

Commission proposal	Drafting suggestions	Comments
controller collects a low amount of personal data, it should be reasonable to expect, for instance, that the data subject has the information on the identity and contact details of the controller as well as on the purpose of the processing when that processing is carried out for the performance of a contract to which a data subject is a party, or when the data subject has given his or her consent to that processing, in accordance with the requirements laid down in Regulation (EU) 2016/679. The same should apply to associations and sport clubs where the processing of personal data is confined to the management of membership, communication with members and the organisation of activities. Nevertheless, this derogation from the obligations of Article 13 is without prejudice to the independent obligations of the controller under Article 15 of that Regulation, which applies in case the data subject requests access based on the latter provision. Where the derogation from the obligations of Article 13 does not apply, in order to balance the need for completeness and easy understanding by the data subject, controllers may adopt a layered approach when providing the information required, notably by allowing users to navigate to further information.		
(37) Where the processing takes place for the purpose of scientific research and the provision of information to the data subject proves to be impossible or would involve a disproportionate		

Commission proposal	Drafting suggestions	Comments
effort it should not be necessary to provide the information provided for under Article 13 of this Regulation. The controller should make reasonable efforts to acquire contact details if they are readily available and acquisition would not require a disproportionate effort. The provision of the information would involve a disproportionate effort in particular where the controller at the time of collection of the personal data did not know or anticipate that it would process personal data for scientific research purposes at a later stage, in which case it may not have easily available contact details of the data subjects. In such situations the controller should inform data subjects indirectly, such as by making the information publicly available. The provision of such information should ensure that as many data subjects concerned as possible are reached. Relevant means to make the information publicly available should be determined depending on the context of the research project and the data subjects involved.		
(38) Article 22 of Regulation (EU) 2016/679 provides for rules governing the processing of personal data when the data controller makes decisions which have legal effects or similarly significant effects on the data subject, based solely on automated processing. In order to provide greater legal certainty, it should be clarified that decisions based solely on automated processing are allowed when specific conditions are met, as set		

Commission proposal	Drafting suggestions	Comments
out in Regulation (EU) 2016/679. It should also be clarified that when assessing whether a decision is necessary for entering into, or performance of, a contract between the data subject and a data controller, as set out in Article 22(2)(a) of Regulation (EU) 2016/679, it should not be required that the decision could be taken only by solely automated processing. This means that the fact that the decision could also be taken by a human does not prevent the controller from taking the decision by solely automated processing When several equally effective automated processing solutions exist, the controller should use the less intrusive one.		
(39) In order to reduce the burden on controllers while ensuring that supervisory authorities have access to the relevant information and can act on violations of the Regulation, the threshold for notification of a personal data breach to the supervisory authority under Article 33 of Regulation (EU) 2016/679 should be aligned with that of communication of a personal data breach to the data subject under Article 34 of that Regulation. In the case of a data breach that is not likely to result in a high risk to the rights and freedoms of natural persons, the controller should not be required to notify the competent supervisory authority. The higher threshold for notifying a data breach to the supervisory authority does not affect the obligation of the controller to document the		

Commission proposal	Drafting suggestions	Comments
breach in accordance with paragraph 5 of Article 33 of Regulation (EU) 2016/679, or its obligation to be able to demonstrate its compliance with that Regulation, in accordance with Article 5(2) of that Regulation. In order to facilitate compliance by controllers and a harmonised approach in the Union, the Board should prepare a common template for notifying data breaches to the competent supervisory authority and a common list of circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person. The Commission should take due account of the proposal prepared by the Board and review them, as necessary, prior to adoption. In order to take account of new information security threats, the common template and the list should be reviewed at least every three years and updated where necessary. The lack of a common list of circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person should not affect the obligations of controllers to notify those breaches.		
(40) Article 35 of that Regulation (EU) 2016/679 requires controllers to conduct a data protection impact assessment where the processing of personal data is likely to result in a high risk to the rights and freedoms of natural persons. The supervisory authorities established pursuant to that Regulation are required to establish and make		

Commission proposal	Drafting suggestions	Comments
public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment. In addition, the Regulation provides that supervisory authorities may establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. In order to effectively contribute to the aim of convergence of the economies and to effectively ensure free flow of personal data between Member States, increase legal certainty, facilitate compliance by controllers and ensure a harmonised interpretation of the notion of a high risk to the rights and freedoms of data subjects, a single list of processing operations should be provided at EU level, to replace the existing national lists. In addition, the publication of a list of the type of processing operations for which no data protection impact assessment is required, which is currently optional, should be made mandatory. The lists of processing operations should be prepared by the Board and adopted by the Commission as an implementing act. In order to facilitate compliance by controllers, the Board should also prepare a common template and a common methodology for conducting data protection impact assessments, to be adopted by the Commission as an implementing act. The Commission should take due account of the proposals prepared by the Board and review them, as necessary, prior to adoption. In order to take account of technological developments, the lists and the common template and methodology should		

Commission proposal	Drafting suggestions	Comments
be reviewed at least every three years and updated where necessary.		
(41) Regulation (EU) 2018/1725 of the European Parliament and of the Council[5] applies to the processing of personal data by the Union institutions, bodies, offices and agencies. Directive (EU) 2016/680 of the European Parliament and of the Council[6] applies to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. Regulation (EU) 2018/1725 and Directive (EU) 2016/680 should be brough into alignment with the amendments to Regulation (EU) 2016/679 introduced by this Regulation. 5 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj). 6 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal		

Commission proposal	Drafting suggestions	Comments
offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89, ELI: http://data.europa.eu/eli/dir/2016/680/oj).		
(42) As clarified in recital 5 of Regulation (EU) 2018/1725, whenever the provisions of Regulation (EU) 2018/1725 follow the same principles as the provisions of Regulation (EU) 2016/679, those two sets of provisions should, under the case law of the Court of Justice of the European Union, be interpreted homogeneously. The scheme of Regulation (EU) 2018/1725 should be understood as equivalent to the scheme of Regulation (EU) 2016/679. Therefore, this Regulation also amends the provisions of Regulation (EU) 2018/1725 that are concerned by the amendments of Regulation (EU) 2016/679, insofar as the latter amendments are also relevant in the context of the processing of personal data by the Union institutions, bodies, offices and agencies.		
(43) In order to provide a strong and coherent data protection framework in the Union, the necessary adaptations of Directive (EU) 2016/680 and any other Union legal act applicable to such processing of personal data should follow after the adoption of this regulation, in order to allow for their application as close as possible to the entry		

Commission proposal	Drafting suggestions	Comments
into application of the amendments to Regulation (EU) 2016/679 and Regulation (EU) 2018/1725.		
(44) The storing of personal data, or the gaining of access to personal data already stored, in a terminal equipment and the subsequent processing of such data should be regulated under a single legal framework, namely Regulation (EU) 2016/679, where the subscriber of the electronic communications service or the user of the terminal equipment is a natural person. The amendments presented in this Regulation continue to offer the highest levels of protection for personal data, while simplifying the experiences of data subjects in exerting their rights and expressing their choices online. The amendments concern in particular storage of information in that equipment, accessing or otherwise collecting information from that equipment that entails the processing of personal data through cookies or similar technologies to gain information from the terminal equipment. The relevant rules should also apply regardless of whether the terminal equipment is owned by the natural person or by another legal or natural person.		
The storing of personal data, or the gaining of access to personal data already stored, in a terminal equipment should continue to be allowed only on the basis of consent. Similar to the approach in		

Commission proposal	Drafting suggestions	Comments
Directive 2002/58/EC, this requirement should not preclude storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person, when that is based on Union or Member State law within the meaning of Article 6 of Regulation (EU) 2016/679 and if it fulfils all conditions of lawfulness laid down in that provision, and is done for the objectives laid down in Article 23(1) of Regulation (EU) 2016/679.		
With a view to reducing the compliance burden and providing legal clarity to controllers, and given that certain purposes of processing pose a low risk to the rights and freedoms of data subjects or that such processing may be necessary to provide a service requested by the data subject, it is necessary to define a limitative list of purposes for which the processing should be permitted without consent. As regards storing of personal data, or the gaining of access to personal data already stored, in a terminal equipment, and subsequent processing that is necessary for those purposes, this Regulation should therefore provide that the processing is lawful. The controller, such as a media service provider, may mandate a processor, such as a market research company, to carry out the processing on its behalf.		

Commission proposal	Drafting suggestions	Comments
For the subsequent processing of personal data for other purpose than those defined in the limitative list, Article 6 and, where relevant, Article 9 of Regulation (EU) 2016/679 should be applied. It is the responsibility of the controller in the light of the principle of accountability to choose the appropriate legal basis for the intended processing. In order to be able to rely on legitimate interest under Article 6(1), point f, of Regulation (EU) 2016/679 as a ground for the subsequent processing of personal data, the controller must show that it pursues the controller's or third parties' legitimate interest, the processing is necessary in order to achieve the purpose of that legitimate interest, and the interests or fundamental rights of the data subject do not override the interests pursued by the controller. In this context, controllers should take outmost account of the following elements: whether the data subject is a child; the reasonable expectations of data subject; the impact on the individual either because of the scale of data processed or the sensitivity of the data processed; the scale of the processing at issue in the sense that the processing cannot be particularly extensive either because of their amount or the range of categories of data; the processing should be based on data limited to what is necessary and cannot be based on monitoring of large parts of the online activity of the data subjects; and other relevant factors as appropriate. The processing		

Commission proposal	Drafting suggestions	Comments
should not give rise to the continuous monitoring of the data subject's private life.		
Where the controller cannot rely on legitimate interest as a legal ground for the subsequent processing, the processing should be based on another ground in Article 6(1), in particular on consent in accordance with Articles 6 and 7 of Regulation (EU) 2016/679, provided that all principles of Regulation (EU) 2016/679 are met.		
(45) Data subjects that have refused a request for consent are often confronted with a new request to give consent each time they visit the same controller's online service again. This may have detrimental effects to the data subjects which may consent just in order to avoid repeating requests. The controller should therefore be obliged to respect the data subject's choices to refuse a request for consent for at least a certain period.		
(46) Data subjects should have the possibility to rely on automated and machine-readable indications of their choice to consent or refuse a consent request or object to the processing of data. Such means should follow the state of the art. They can be implemented in the settings of a web browser or in the EU Digital Identity Wallet as set out by Regulation (EU) 914/2014, or any other adequate means. Rules set out in this Regulation		

Commission proposal	Drafting suggestions	Comments
should support the emergence of market-driven solutions with appropriate interfaces. The controller should be obliged to respect automated and machine-readable indications of data subject's choices once there are available standards. In light of the importance of independent journalism in a democratic society and in order not to undermine the economic basis for that, media service providers should not be obliged to respect the machine-readable indications of data subject's choices. The obligation for providers of web browsers to provide the technical means for data subjects to make choices with respect to the processing should not undermine the possibility for media service providers to request consent by data subjects.		
(47) Directive 2002/58/EC on privacy and electronic communications 'ePrivacy Directive'), last revised in 2009, provides a framework for the protection of the right to privacy, including the confidentiality of communications. It also specifies Regulation (EU) 2016/679 in relation to processing of personal data in the context of electronic communication services. It protects the privacy and the integrity of user's or subscriber's terminal equipment used for such communications. The current provision of Article 5(3) of Directive 2002/58/EC should remain applicable insofar as the subscriber or user is not a natural person, and the information stored or accessed does not		

Commission proposal	Drafting suggestions	Comments
constitute or lead to the processing of personal data.		
(48) Article 4 of Directive 2002/58/EC should be repealed. Article 4 of Directive 2002/58/EC sets requirements for providers of publicly available electronic communications services as regards safeguarding the security of their services and notification requirements. Subsequently, Directive (EU) 2022/2555 has set new requirements as regards cybersecurity risk-management measures and incident reporting for those providers. In order to reduce overlapping obligations for entities in the electronic communications sector, Article 4 of Directive 2002/58/EC should be repealed. As regards the security of processing of personal data pursuant to Article 4(1) and (1a) of this directive and the notification of personal data breaches pursuant to Article 4(3) to (5) of Directive 2002/58/EC this directive, the Regulation (EU) 2016/679 already provide for comprehensive and up-to-date rules. These rules should therefore apply to providers of publicly available electronic communication services and providers of public communications networks, thereby ensuring that one regime applies to the controllers and processors.	(48) ~~Article 4 of Directive 2002/58/EC should be repealed.~~ Article 4 of Directive 2002/58/EC sets requirements for providers of publicly available electronic communications services as regards safeguarding the security of their services and notification requirements. Subsequently, Directive (EU) 2022/2555 has set new requirements as regards cybersecurity risk-management measures and incident reporting for those providers. In order to reduce overlapping obligations for entities in the electronic communications sector, Article 4 of Directive 2002/58/EC should be repealed.	CZ: the first sentence of this recital is repetitive with latter one in the same point, and therefore seems to be redundant and should be deleted.
[…]		

Commission proposal	Drafting suggestions	Comments
(59) Regulation (EU) 2019/1150 establishes a targeted set of mandatory rules at Union level to ensure a fair, predictable, sustainable and trusted online business environment within the internal market. Regulation (EU) 2022/2065 and Regulation (EU) 2022/1925 provide a comprehensive regulatory framework for a safe, predictable and trusted online environments for all end-users of online services, and establish a level playing field for businesses in digital markets. In the interest of simplification of Union legislation in the field of online intermediation services and online platforms, and given that the objectives and material provisions of the Platform-to-Business Regulation are largely covered by the Digital Services Act and the Digital Markets Act, Regulation (EU) 2019/1050 should be repealed. Regulation (EU) 2022/2065 and Regulation (EU) 2022/1925 contribute to a fully harmonised regulatory framework for digital services and digital markets, by approximating national measures concerning the requirements for providers of intermediary services and the contestability and fairness of core platforms services provided by gatekeepers. For purposes of legal certainty, selected definitions in Article 2, the provisions on restrictions and suspensions in Article 4, as well as on the internal complaint-handling system in Article 11 of Regulation (EU) 2019/1150 that are cross-referenced by other legal acts, in particular Directive (EU) 2023/2831 on improving working conditions in platform work,		

Commission proposal	Drafting suggestions	Comments
and Article 15 ensuring enforcement, will temporarily remain in application until the original acts are amended.		
[…]		
HAVE ADOPTED THIS REGULATION:		
[…]		
Article 3		
Amendments to Regulation (EU) 2016/679 (GDPR)		
Regulation (EU) 2016/679 is amended as follows:		
1. Article 4 is amended as follows:		
	1. Article 2 paragraph 4 is amended as follows: **´4. This Regulation shall be without prejudice to the application of Regulation (EU) 2022/2065, in particular liability under this Regulation shall not prevail over the liability**	CZ proposes two elements: **1. update of the link to DSA, instead of eCommerce directive.** This is to make the reading easier by incorporating the rule of Article 89 DSA.

Commission proposal	Drafting suggestions	Comments
	rules applicable to intermediary service providers as set out in Articles Articles 4, 5, 6 and 8 of thas Regulation.'	**2. explicit explanation to the interplay of liability rules between GDPR and DSA** CZ considers that the conclusions drawn from the judgment of the Court of Justice of 2 December 2025, case C-492/23, X v Russmedia Digital SRL and Inform Media Press SRL, are systemic and potentially risky for the functioning of the European digital economy. Liability exemptions and principle of no general monitoring or active fact-finding obligations under the e-Commerce Directive (or consequently the DSA Regulation) are general rules and a prerequisites for the free functioning of digital platforms. If these rules were to be suppressed in favor of liability under the Regulation (EU) 2016/679, these platforms would be directly liable for certain illegal user-generated content. If platforms were directly liable for illegal user-generated content, they would not be able to carry out their activities without a reasonable risk of being punished for doing so, even though they operate reasonably and with a sincere effort to comply with all their legal obligations. Currently, there is no technical way to operate a platform in such a way that the provider can be absolutely

Commission proposal	Drafting suggestions	Comments
		certain that no illegal user-generated content will be stored on their platform. The proposed amendment does not bring about a drastic change in the current legal situation, but rather specifies and assures that platforms can conduct their business in a similar manner to how they have since the e-Commerce Directive and the DSA Regulation came into force. The proposed amendment thus increases legal certainty and predictability for providers of digital platforms and ensures that those providers are not forced to actively monitor all user-generated content stored on their platforms.
(a) in point 1, the following sentences are added:	~~(a) in point 1, the following sentences are added:~~	CZ: prefers other more suitable means of more precise definition of identifiability, which would not unproportionately decrease legal certainty.
'Information relating to a natural person is not necessarily personal data for every other person or entity, merely because another entity can identify that natural person. Information shall not be personal for a given entity where that entity cannot identify the natural person to whom the information relates, taking into account the means reasonably likely to be used by that entity. Such information does not become personal for that entity merely because a potential subsequent recipient has means reasonably likely to be used to	~~'Information relating to a natural person is not necessarily personal data for every other person or entity, merely because another entity can identify that natural person. Information shall not be personal for a given entity where that entity cannot identify the natural person to whom the information relates, taking into account the means reasonably likely to be used by that entity. Such information does not become personal for that entity merely because a potential subsequent recipient has means reasonably likely to be used~~	

Commission proposal	Drafting suggestions	Comments
identify the natural person to whom the information relates.'	~~to identify the natural person to whom the information relates.'~~	
(b) the following points are added:		
'(32) 'terminal equipment' means terminal equipment as set out in Article 1(1) of Directive 2008/63/EC;		
(33) for 'electronic communications networks' the definition of Article 2(1) of Directive (EU) 2018/1972 shall apply;		
(34) 'web browser' means web browser as defined in Article 2(11) of Regulation (EU) 2022/1925;		
(35) 'media service' means a media service as defined in Article 2(1) of Regulation (EU) 2024/1083;		
(36) 'media service provider' means a media service provider as defined in Article 2(2) of Regulation (EU) 2024/1083;'		

Commission proposal	Drafting suggestions	Comments
(37) 'online interface' means an online interface as defined in Article 3(m) of Regulation (EU) 2022/2065.'		
(38) "scientific research" means any research which can also support innovation, such as technological development and demonstration. These actions shall contribute to existing scientific knowledge or apply existing knowledge in novel ways, be carried out with the aim of contributing to the growth of society´s general knowledge and wellbeing and adhere to ethical standards in the relevant research area. This does not exclude that the research may also aim to further a commercial interest.'	(38) "scientific research" means any research which can also support innovation, such as technological development and demonstration. These actions shall contribute to existing scientific knowledge or apply existing knowledge in novel ways, be carried out with the aim of contributing to the growth of society´s general knowledge and wellbeing and adhere to ethical standards, **including scientific methods**, in the relevant research area. This does not exclude that the research may also aim to further a commercial interest.'	CZ: Scientific research is foremostly defined by using scientific methods, which should be explicitly mentioned.
2. Article 5 (1)(b) is replaced by the following:		
'collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), be considered to be compatible with the initial purposes, independent of the conditions of Article 6(4) of this Regulation, ('purpose limitation');'		

Commission proposal	Drafting suggestions	Comments
	2a. Article 6a is added: **Article 6a** ***Processing in the context of the development and operation of AI*** **Where the processing of personal data is necessary for the interests of the controller in the context of the development and operation of an AI system as defined in Article 3, point (1), of Regulation (EU) 2024/1689 or an AI model, such processing may be pursued for legitimate interests within the meaning of Article 6(1)(f) of Regulation (EU) 2016/679, where appropriate, except where other Union or national laws explicitly require consent, and where such interests are overridden by the interests, or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.** **Any such processing shall be subject to appropriate organisational, technical measures and safeguards for the rights and freedoms of the data subject, such as to ensure respect of data minimisation during the stage of selection of sources and the training and testing of AI an system or AI model, to protect against non-disclosure of residually retained data in the AI system or AI model to ensure enhanced transparency to data subjects and providing**	CZ: If adopted, Article 88c GDPR should be moved to Article 6a GDPR, where it fits more systematically. It regulates the legal basis for processing personal data for AI purposes.

Commission proposal	Drafting suggestions	Comments
	data subjects with an unconditional right to object to the processing of their personal data.'	
3. Article 9 is amended as follows:		
(a) in paragraph 2, the following points are added:		
'(k) processing in the context of the development and operation of an AI system as defined in Article 3, point (1), of Regulation (EU) 2024/1689 or an AI model, subject to the conditions referred to in paragraph 5.		
(l) processing of biometric data is necessary for the purpose of confirming the identity of a data subject (verification), where the biometric data or the means needed for the verification is under the sole control of the data subject.'		
(b) the following paragraph is added:		
'5. For processing referred to in point (k) of paragraph 2, appropriate organisational and technical measures shall be implemented to avoid v the collection and otherwise processing of special categories of personal data. Where, despite the implementation of such measures, the controller		

Commission proposal	Drafting suggestions	Comments
identifies special categories of personal data in the datasets used for training, testing or validation or in the AI system or AI model, the controller shall remove such data. If removal of those data requires disproportionate effort, the controller shall in any event effectively protect without undue delay such data from being used to produce outputs, from being disclosed or otherwise made available to third parties.'		
4. In Article 12, paragraph 5 is replaced by the following:		
'5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character or also, for requests under Article 15 because the data subject abuses the rights conferred by this regulation for purposes other than the protection of their data, the controller may either:		
(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or		

Commission proposal	Drafting suggestions	Comments
(b) refuse to act on the request.		
The controller shall bear the burden of demonstrating that the request is manifestly unfounded or that there are reasonable grounds to believe that it is excessive.'		
5. In Article 13, paragraph 4 is replaced by the following:		
'4. Paragraphs 1, 2 and 3 shall not apply where the personal data have been collected in the context of a clear and circumscribed relationship between data subjects and a controller exercising an activity that is not data-intensive and there are reasonable grounds to assume that the data subject already has the information referred to in points (a) and (c) of paragraph 1, unless the controller transmits the data to other recipients or categories of recipients, transfers the data to a third country, carries out automated decision-making, including profiling, referred to in Article 22(1), or the processing is likely to result in a high risk to the rights and freedoms of data subjects within the meaning of Article 35.'		
6. In Article 13, paragraph 5 is added:		

Commission proposal	Drafting suggestions	Comments
'5. When the processing takes place for scientific research purposes and the provision of information referred to under paragraphs 1, 2 and 3 proves impossible or would involve a disproportionate effort subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing, the controller does not need to provide the information referred to under paragraphs 1, 2 and 3. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available.'		
7. In Article 22, paragraphs 1 and 2 are replaced by the following:		
'1. A decision which produces legal effects for a data subject or similarly significantly affects him or her may be based solely on automated processing, including profiling, only where that decision:	1. 1. ~~A decision which produces legal effects for a data subject or similarly significantly affects him or her may be based solely on automated processing, including profiling, only where that decision~~ **The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.**	CZ: CZ supports the amendment of point (a), but wonders why the change of structure of this Article is necessary.

Commission proposal	Drafting suggestions	Comments
	2. Paragraph 1 shall not apply if the decision:	
(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller regardless of whether the decision could be taken otherwise than by solely automated means;	(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller regardless of whether the decision could be taken otherwise than by solely automated means;	
(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or		
(c) is based on the data subject's explicit consent.'		
8. Article 33 is amended as follows:		
(a) paragraph 1 is replaced by the following:		
'1. In the case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall without undue delay and, where feasible, not later than 96 hours after having become aware of it,	1. In the case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall without undue delay and, where feasible, not later than 96 hours after having become aware of it, notify the personal data breach via the single-entry point established	CZ: Simplification intended primarily for small controllers processing data within single Member State not affecting significantly data subjects in other Member States (i.e. excluding cases under Art. 4 point 23 GDPR).

Commission proposal	Drafting suggestions	Comments
notify the personal data breach via the single-entry point established pursuant to Article 23a of Directive (EU) 2022/2555 to the supervisory authority competent in accordance with Article 55 and Article 56. Where the notification to the supervisory authority is not made within 96 hours, it shall be accompanied by reasons for the delay.'	pursuant to Article 23a of Directive (EU) 2022/2555 to the supervisory authority competent in accordance with Article 55 and Article 56. **However, where such a personal data breach does not concern cross-border processing, the controler may notify a personal data breach directly to the competent supervisory authority.** Where the notification to the supervisory authority is not made within 96 hours, it shall be accompanied by reasons for the delay.	
(b) the following paragraph is added:		
'1a. Until the establishment of the single-entry point pursuant to Article 23a of Directive (EU) 2022/2555, controllers shall continue to notify personal data breaches directly to the competent supervisory authority in accordance with Article 55 and Article 56.'		
(c) the following paragraphs are added:		
'6. The Board shall prepare and transmit to the Commission a proposal for a common template for notifying a personal data breach to the competent supervisory authority referred to in paragraph 1 as well as for a list of the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person. The		

Commission proposal	Drafting suggestions	Comments
proposals shall be submitted to the Commission within [OP date = nine months of the entry into application of this Regulation]. The Commission after due consideration reviews it, as necessary, and is empowered to adopt it by way of an implementing act in accordance with the examination procedure set out in Article 93(2).		
7. The template and the list referred to in paragraph 6 shall be reviewed at least every three years and updated where necessary. The Board shall submit its assessment and possible proposals for updates to the Commission in due time. The Commission after due consideration of the proposals reviews them and is empowered to adopt any updates following the procedure in paragraph 6.'		
9. Article 35 is amended as follows:		
(a) paragraphs 4, 5 and 6 are replaced by the following:		
'4. The Board shall prepare and transmit to the Commission a proposal for a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1.		CZ: CZ supports EU-wide lists. However, complementary national lists should be possible to address local, specific or emerging issues – see the proposal of new Art. 35 para 6d.

Commission proposal	Drafting suggestions	Comments
5. The Board shall prepare and transmit to the Commission a proposal for a list of the kind of processing operations for which no data protection impact assessment is required.		
6. The Board shall prepare and transmit to the Commission a proposal for a common template and a common methodology for conducting data protection impact assessments.'		
(b) the following paragraphs are inserted:		
'6a. The proposals for the lists referred to in paragraphs 4 and 5 and for the template and methodology referred to in paragraph 6 shall be submitted to the Commission within [OP date = 9 months of the entry into application of this Regulation]. The Commission after due consideration reviews them, as necessary, and is empowered to adopt them by way of an implementing act in accordance with the examination procedure set out in Article 93(2).		
6b. The lists and the template and methodology referred to in paragraph 6a- shall be reviewed at least every three years and updated where necessary. The Board shall submit its assessment		

Commission proposal	Drafting suggestions	Comments
and possible proposals for updates to the Commission in due time. The Commission after due consideration of the proposals reviews them and is empowered to adopt any updates following the procedure in paragraph 6a.		
6c. Lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment and of the kind of processing operations for which no data protection impact assessment is required established and made public by supervisory authorities remain valid until the Commission adopts the implementing act referred to in paragraph 6a.'	6c. Lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment and of the kind of processing operations for which no data protection impact assessment is required established and made public by supervisory authorities remain valid until the Commission adopts the implementing act referred to in paragraph 6a. **6d. The supervisory authority may establish and make public lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment and of the kind of processing operations for which no data protection impact assessment is required only where such lists are not in contravention of the lists adopted following the procedure in paragraph 6a. The supervisory authority shall communicate those lists to the Commission.**	CZ: CZ supports EU-wide lists. However, complementary national lists should be possible to address local, specific or emerging issues.
10. The following article is added:	~~10. The following article is added:~~	CZ: CZ is of the opinion that such fundamental elements of regulation of data protection should not be left to implementing acts, but if considered necessary, rather that the basic criteria be explicitly regulated in GDPR.

Commission proposal	Drafting suggestions	Comments
‘Article 41a		
(1) The Commission may adopt implementing acts to specify means and criteria to determine whether data resulting from pseudonymisation no longer constitutes personal data for certain entities.		CZ: CZ understands that implementing acts should not directly determine the notion of personal data. However, the ability to determine where pseudonymised data are no longer personal data for certain entities is - albeit indirect and relative - delimitation of the notion of personal data, which is a basic element of the GDPR. Therefore, CZ believes that this Article should, at the very least, include the core requirements on the means and criteria, similar to core requirements on adequacy decisions. Additionally, the scope of Art 83(4)(a) should be extended as follows: “the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39**, 41a** and 42 and 43”. - depends on the final wording of Article 41a. Should be ommitted where Article 41a would not actually provide for obligations for controllers and/or recipients (in the original proposal, obligation to assess is implied in Art. 41a(2)(b).
(2) For the purpose of paragraph 1 the Commission shall:		
(a) assess the state of the art of available techniques;		

Commission proposal	Drafting suggestions	Comments
(b) develop criteria and or categories for controllers and recipients to assess the risk of re-identification in relation to typical recipients of data.		
(3) The implementation of the means and criteria outlined in an implementing act may be used as an element to demonstrate that data cannot lead to reidentification of the data subjects.		
(4) The Commission shall closely involve the EDPB in the preparations of the implementing acts. The EPDB shall issue an opinion on the draft implementing acts within a deadline of 8 weeks as of the receipt of the draft from the Commission.		
(5) The Implementing Acts shall be adopted in accordance with the examination procedure referred to in Article 93(3).'		
11. In Article 57(1) is amended as follows:		
(a) point (k) is deleted;		
12. In Article 64(1), point (a) is deleted.		

Commission proposal	Drafting suggestions	Comments
13. In Article 70(1), point (h) is deleted.		
14. In Article 70(1), the following points are inserted:		
‘(ha) prepare and transmit to the Commission a proposal for a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment and for which no data protection impact assessment is required, pursuant to Article 35.		
(hb) prepare and transmit to the Commission a proposal for a common template and a common methodology for conducting data protection impact assessments, pursuant to Article 35.		
(hc) prepare and transmit to the Commission a proposal for a common template for notifying a personal data breach to the competent supervisory authority as well as for a list of the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person pursuant to Article 33’		
	14a. In Article 77 paragraph 3 is added:	CZ: The aim of detailed rules for handling of complaints lies in the possibility of prioritising and planning regulatory action based on the actual

Commission proposal	Drafting suggestions	Comments
	3. Member States may incorporate into their national law rules for prioritisation of complaints based on reviewable and publicly available criteria.	impact of complaints and the resources available. Prioritisation shall be based on reviewable and publicly available criteria, without prejudice to the obligation to provide a reasoned effective response and subject to judicial review in every case. The powers of supervisory authorities to adopt planning instruments for the prioritisation and management of complaints should be expressly recognised. This would enable the DPAs more targeted supervisory activities based on evaluation of the level of risk, affects, type of processing, sector etc., while maintaining the capacity for individual assessment of each case. Priority should be given in particular to complaints that demonstrate a clear link to the core right to data protection or a high risk to rights and freedoms, affect many data subjects as well as other criteria.
15. After Article 88, the following articles are added:	New point (f) should be added to Art. 83(5) "**specific processing situations pursuant to Articles 88a to 88c."**	CZ: Additionally, the scope of Art 83(5) should be extended and new point (f) should be added: "**specific processing situations pursuant to Articles 88a to 88c.** " These provisions are different from other articles on specific processing situations, because these provisions do not rely on Member State law. Therefore, the sanctions for breaches of Art. 88a-88c should be stipulated in the GDPR. We stress that the scope of Art. 83 GDPR does not cover Articles 88a to 88c, because of how the Art. 83(4)(5) GDPR are worded. These provisions are different from other GDPR articles on specific processin situations, because

Commission proposal	Drafting suggestions	Comments
		these newly proposed provisions do not rely on Member State law. Therefore, sanctions for infringements of Art. 88a-88c should be stipulated in the GDPR. CZ suggests adding new Art. 83(5)(f), but is flexible as regards the exact solutions. That is especially because it should also be clarified which entities obliged under Art. 88a-88c (or 41a) should be subject to GDPR enforcement, in particular whether other powers of DPAs in Art. 58 should be adapted to new situations / entities.
‘Article 88a		
Processing of personal data in the terminal equipment of natural persons	*Processing of personal data in the terminal equipment of natural persons* **in connection with the provision of publicly available electronic communications services in public communications networks**	CZ: To clarify that the scope of these provisions should not be interpreted broader than in e-Privacy Directive.
(1) Storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person is only allowed when that person has given his or her consent, in accordance with this Regulation.	(1) Storing of personal data, or gaining of access to personal data already stored, **in connection with the provision of publicly available electronic communications services in public communications networks (‘personal communication data’)** in the terminal equipment of a natural person is only allowed when that	CZ**:** The proposed wording, considering the unclear scope of application (the meaning of “personal data already stored in the terminal equipment” in the context of GDPR as a general regulation of personal data proceesing as opposed to e-Privacy Directive, i.e. the processing of personal data in electronic communications), is too

Commission proposal	Drafting suggestions	Comments
	person has given his or her consent, in accordance with this Regulation.	far-reaching. The scope and limits of the provision as formulated in this way are unclear. Such an approach could allow for blanket surveillance and interference with the privacy of end-users, contrary to Articles 7 and 8 of the Charter and the case-law of the Court of Justice. Following the clarification of the scope of the provision the wording shall be amended to include proper safeguards.
(2) Paragraph 1 does not preclude storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person, based on Union or Member State law within the meaning of, and subject to the conditions of Article 6, to safeguard the objectives referred to in Article 23(1).	(2) Paragraph 1 does not preclude storing of personal **communication** data, or gaining of access to personal **communication** data already stored, in the terminal equipment of a natural person, based on Union or Member State law within the meaning of, and subject to the conditions of Article 6, to safeguard the objectives referred to in Article 23(1), **subject to conditions set in Article 23 that shall apply *mutatis mutandis*.**	CZ: First, precise definition of relevant personal data is taken over from paragraph 1 by using short phrase. Second, reference to "objectives referred to in Article 23(1)" should be supplemented by reference to the safeguards provided for by Article 23. These safeguards include the legislative nature of a measure, the respect of the essence of the fundamental rights and freedoms and the necessity and proportionality requirements in paragraph 1, and concrete elements of the legislative measure required by paragraph 2 where relevant. Third, because the Article 23(1) refers to limitation of particular rights provided in specific provisions of GDPR, the reference should be to conditions that apply "mutatis mutandis". Legislative technique of Regulation 2019/1381 is used.
(3) Storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person without	(3) Storing of personal **communication** data, or gaining of access to personal **communication** data already stored, in the terminal equipment of a	CZ: Precise definition of relevant personal data is taken over from paragraph 1 by using the shortened phrase.

Commission proposal	Drafting suggestions	Comments
consent, and subsequent processing, shall be lawful to the extent it is necessary for any of the following:	natural person without consent, and subsequent processing, shall be lawful to the extent it is necessary for any of the following:	
(a) carrying out the transmission of an electronic communication over an electronic communications network;		
(b) providing a service explicitly requested by the data subject;		
(c) creating aggregated information about the usage of an online service to measure the audience of such a service, where it is carried out by the controller of that online service solely for its own use;		
(d) maintaining or restoring the security of a service provided by the controller and requested by the data subject or the terminal equipment used for the provision of such service.		CZ: The addition of letter (d) on security of a service raised some concerns. CZ trusts this should be solved by adding the **legal ground** related to the formulation of this point or make the text more specific by **giving examples.** Such clarification shall be reflected in the normative text of the regulation. Security of the service provided by the controller: Anti-fraud and anomaly detection: Storing identifiers to detect suspicious behavior (e.g.,

Commission proposal	Drafting suggestions	Comments
		unusual login from another country, changes in behavior patterns indicating account compromise) Rate limiting: Cookies/fingerprinting to protect against DDoS attacks and brute-force login attempts CSRF tokens: Protection of forms against cross-site request forgery and similar attacks Session integrity: Control mechanisms to detect "session hijacking" or "session fixation" Bot detection: Identification of automated access threatening service availability Security of the end user's device: Phishing warning: Systems warning users about compromise of their devices TLS/certificate verification: Data necessary to verify secure connection Important note: The "necessity" test must be met - an alternative solution without access to personal data would not be sufficiently effective. And the service must be "requested" by the data subject.
(4) Where storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person is based on consent, the following shall apply:	(4) Where storing of personal **communication** data, or gaining of access to personal **communication** data already stored, in the terminal equipment of a natural person is based on consent, the following shall apply:	CZ: Precise definition of relevant personal data is taken over from paragraph 1 by using the shortened phrase.
(a) the data subject shall be able to refuse requests for consent in an easy and intelligible		

Commission proposal	Drafting suggestions	Comments
manner with a single-click button or equivalent means;		
(b) if the data subject gives consent, the controller shall not make a new request for consent for the same purpose for the period during which the controller can lawfully rely on the consent of the data subject;		
(c) if the data subject declines a request for consent, the controller shall not make a new request for consent for the same purpose for a period of at least six months.		
This paragraph also applies to the subsequent processing of personal data based on consent.	This paragraph also applies to the subsequent processing of personal **communication** data based on consent.	CZ: Precise definition of relevant personal data is taken over from paragraph 1 by using the shortened phrase.
(5) This Article shall apply from [OP: please insert the date = 6 months following the date of entry into force of this Regulation]		
Article 88b		
Automated and machine-readable indications of data subject's choices with respect to processing	*Automated and machine-readable indications of data subject's choices with respect to processing of personal **communication** data in the terminal equipment of natural persons*	CZ: Precise definition of relevant personal data is taken over from paragraph 1 by using the shortened phrase.

Commission proposal	Drafting suggestions	Comments
of personal data in the terminal equipment of natural persons		
(1) Controllers shall ensure that their online interfaces allow data subjects to:		
(a) Give consent through automated and machine-readable means, provided that the conditions for consent laid down in this Regulation are fulfilled;		
(b) decline a request for consent and exercise the right to object pursuant to Article 21(2) through automated and machine-readable means.		
(2) Controllers shall respect the choices made by data subjects in accordance with paragraph 1.		
(3) Paragraphs 1 and 2 shall not apply to controllers that are media service providers when providing a media service.		
(4) The Commission shall, in accordance with Article 10(1) of Regulation (EU) 1025/2012, request one or more European standardisation organisations to draft standards for the		

Commission proposal	Drafting suggestions	Comments
interpretation of machine-readable indications of data subjects' choices.		
Online interfaces of controllers which are in conformity with harmonised standards or parts thereof the references of which have been published in the *Official Journal of the European Union* shall be presumed to be in conformity with the requirements covered by those standards or parts thereof, set out in paragraph 1.		
(5) Paragraphs 1 and 2 shall apply from [OP: please insert the date = 24 months following the date of entry into force of this Regulation].		
(6) Providers of web browsers, which are not SMEs, shall provide the technical means to allow data subjects to give their consent and to refuse a request for consent and exercise the right to object pursuant to Article 21(2) through the automated and machine-readable means referred to in paragraph 1 of this Article, as applied pursuant to paragraphs 2 to 5 of this Article.		
(7) Paragraph 6 shall apply from [OP: please insert the date = 48 months following the date of entry into force of this Regulation].		

Commission proposal	Drafting suggestions	Comments
Article 88c	~~Article 88c~~	CZ: If adopted, Article 88c GDPR should be moved to Article 6a GDPR, where it fits more systematically. The wording needs to be further clarified, e.g. it shall be made clear that controllers can lawfully rely on Article 6(1)(f) GDPR provided that all conditions of that provision are met (carry out the three-step case-by-case assessment). The specific right to object in the context of of the development and operation of AI shall be rather added to Article 21 GDPR.
Processing in the context of the development and operation of AI	~~*Processing in the context of the development and operation of AI*~~	
Where the processing of personal data is necessary for the interests of the controller in the context of the development and operation of an AI system as defined in Article 3, point (1), of Regulation (EU) 2024/1689 or an AI model, such processing may be pursued for legitimate interests within the meaning of Article 6(1)(f) of Regulation (EU) 2016/679, where appropriate, except where other Union or national laws explicitly require consent, and where such interests are overridden by the interests, or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.	~~Where the processing of personal data is necessary for the interests of the controller in the context of the development and operation of an AI system as defined in Article 3, point (1), of Regulation (EU) 2024/1689 or an AI model, such processing may be pursued for legitimate interests within the meaning of Article 6(1)(f) of Regulation (EU) 2016/679, where appropriate, except where other Union or national laws explicitly require consent, and where such interests are overridden by the interests, or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.~~	
Any such processing shall be subject to appropriate organisational, technical measures and safeguards	~~Any such processing shall be subject to appropriate organisational, technical measures and safeguards for the rights and freedoms of the data subject, such~~	

Commission proposal	Drafting suggestions	Comments
for the rights and freedoms of the data subject, such as to ensure respect of data minimisation during the stage of selection of sources and the training and testing of AI an system or AI model, to protect against non-disclosure of residually retained data in the AI system or AI model to ensure enhanced transparency to data subjects and providing data subjects with an unconditional right to object to the processing of their personal data.'	~~as to ensure respect of data minimisation during the stage of selection of sources and the training and testing of AI an system or AI model, to protect against non-disclosure of residually retained data in the AI system or AI model to ensure enhanced transparency to data subjects and providing data subjects with an unconditional right to object to the processing of their personal data.'~~	
Article 4		
Amendments to Regulation (EU) 2018/1725 (EUDPR)		
Regulation (EU) 2018/1725 is amended as follows:		
1. Article 3 is amended as follows:		
(a) in point 1, the following sentences are added:		
'Information relating to a natural person is not necessarily personal data for every other person or entity, merely because another entity can identify that natural person. Information shall not be personal for a given entity where that entity cannot		

Commission proposal	Drafting suggestions	Comments
identify the natural person to whom the information relates, taking into account the means reasonably likely to be used by that entity. Such information does not become personal for that entity merely because a potential subsequent recipient has means reasonably likely to be used to identify the natural person to whom the information relates.'		
(b) point 25 is replaced by the following:		
'(25) for 'electronic communications networks' the definition of Article 2(1) of Directive (EU) 2018/1972 shall apply;'		
(c) the following points are added:		
'(27) 'mobile application' means a mobile application as defined in Article 3(2) of Directive (EU) 2016/2102;		
(28) 'online interface' means an online interface as defined in Article 3(m) of Regulation (EU) 2022/2065;		

Commission proposal	Drafting suggestions	Comments
(29) "scientific research" means any research which can also support innovation, such as technological development and demonstration. These actions shall contribute to existing scientific knowledge or apply existing knowledge in novel ways, be carried out with the aim of contributing to the growth of society´s general knowledge and wellbeing and adhere to ethical standards in the relevant research area. This does not exclude that the research may also aim to further a commercial interest.'		
2. Article 4 (1)(b) is replaced by the following:		
'(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 13, be considered to be compatible with the initial purposes, independent of the conditions of Article 6 of this Regulation, ('purpose limitation');'		
3. Article 10 is amended as follows:		

Commission proposal	Drafting suggestions	Comments
(a) in paragraph 2, the following points are added:		
'(k) processing in the context of the development and operation of an AI system as defined in Article 3, point (1), of Regulation (EU) 2024/1689 or an AI model, subject to the conditions referred to in paragraph 4. -		
(l) processing of biometric data is necessary for the purpose of confirming the identity of a data subject (verification), where the biometric data or the means needed for the verification is under the sole control of the data subject.'		
(b) the following paragraph 4 is added:		
'4. For processing referred to in point (k) of paragraph 2, appropriate organisational and technical measures shall be implemented to avoid the collection and otherwise processing of special categories of personal data. Where, despite the implementation of such measures, the controller identifies special categories of personal data in the datasets used for training, testing or validation or in the AI system or AI model, the controller shall remove such data. If removal of those data requires disproportionate effort, the controller shall in any		

Commission proposal	Drafting suggestions	Comments
event effectively protect without undue delay such data from being used to produce outputs, from being disclosed or otherwise made available to third parties.'		
4. in Article 14, paragraph 5 is replaced by the following:		
'5. Information provided under Articles 15 and 16 and any communication and any actions taken under Articles 17 to 24 and 35 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character or also, for requests under Article 17 because the data subject abuses the rights conferred by this Regulation for purposes other than the protection of their data, the controller may refuse to act on the request. The controller shall bear the burden of demonstrating that the request is manifestly unfounded or that there are reasonable grounds to believe that it is excessive.'		
5. in Article 15 the new paragraph 5 is added:		
'5. When the processing takes place for scientific research purposes and the provision of information referred to under paragraphs 1, 2 and 3 proves impossible or would involve a disproportionate		

Commission proposal	Drafting suggestions	Comments
effort subject to the conditions and safeguards referred to in Article 13 or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing, the controller does not need to provide the information referred to under paragraphs 1, 2 and 3. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available.'		
6. in Article 24 paragraphs 1 and 2 are replaced by the following:		
'1. A decision which produces legal effects for a data subject or similarly significantly affects him or her may be based solely on automated processing, including profiling, only where that decision:		
(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller regardless of whether the decision could be taken otherwise than by solely automated means;		

Commission proposal	Drafting suggestions	Comments
(b) is authorised by Union law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or		
(c) is based on the data subject's explicit consent.'		
7. in Article 34, paragraph 1 is replaced by the following		
'1. In the case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall without undue delay and, where feasible, not later than 96 hours after having become aware of it, notify the personal data breach to the European Data Protection Supervisor. Where the notification to the European Data Protection Supervisor is not made within 96 hours, it shall be accompanied by reasons for the delay.'		
8. In Article 37 the following paragraphs are added:		
'(2) Storing of personal data, or gaining of access to personal data already stored, in the terminal		

Commission proposal	Drafting suggestions	Comments
equipment of a natural person is only allowed when that person has given his or her consent, in accordance with this Regulation.		
(3) Paragraph 1 does not preclude storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person, based on Union law within the meaning of, and subject to the conditions of Article 5, to safeguard the objectives referred to in Article 25(1).		
(4) Storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person without consent, and subsequent processing, shall be lawful to the extent it is necessary for any of the following:		
(a) carrying out the transmission of an electronic communication over an electronic communications network;		
(b) providing a service explicitly requested by the data subject;		
(c) creating aggregated information about the usage of an online service to measure the audience of such a service, where it is carried out by		

Commission proposal	Drafting suggestions	Comments
the controller of that online service solely for its own use;		
(d) maintaining or restoring the security of a service provided by the controller and requested by the data subject or the terminal equipment used for the provision of such service.		
(5) Where storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person is based on consent, the following shall apply:		
(a) the data subject shall be able to refuse requests for consent in an easy and intelligible manner with a single-click button or equivalent means;		
(b) if the data subject gives consent, the controller shall not make a new request for consent for the same purpose for the period during which the controller can lawfully rely on the consent of the data subject;		
(c) if the data subject declines a request for consent, the controller shall not make a new request for consent for the same purpose for a period of at least six months.		

Commission proposal	Drafting suggestions	Comments
This paragraph also applies to the subsequent processing of personal data based on consent.		
(6) This Article shall apply from [OP: please insert the date = 6 months following the date of entry into force of this Regulation]]		
(7) Controllers shall ensure that their online interfaces allow data subjects to:		
(a) give consent through automated and machine-readable means, provided that the conditions for consent laid down in this Regulation are fulfilled;		
(b) decline a request for consent through automated and machine-readable means.		
(8) Controllers shall respect the choices made by data subjects in accordance with paragraph 7.		
(9) Online interfaces of controllers which are in conformity with harmonised standards or parts thereof referred to in paragraph 4 of Article 88b of Regulation (EC) 2016/679 shall be presumed to be in conformity with the requirements covered by		

Commission proposal	Drafting suggestions	Comments
those standards or parts thereof, set out in paragraph 7.		
(10) Paragraphs 7 to 9 shall apply from [OP: please insert the date = 24 months following the date of entry into force of this Regulation].		
(8) Article 39 is amended as follows:		
(a) Paragraph 4 is replaced by the following:		
'4. The lists, the template and methodology adopted by the Commission and referred to in paragraph 6a of Article 35 of Regulation (EU) 2016/679 should apply to the processing of personal data under this Regulation.'		
(b) Paragraphs 5 and 6 are deleted.		
(9) the following article is added:		
'Article 45a		
The common criteria adopted by the Commission and referred to in article 41a of the Regulation (EU)		

Commission proposal	Drafting suggestions	Comments
2016/679 should apply to the processing of personal data under this Regulation.'		
Article 5		
Amendments to and Directive 2002/58/EC (ePrivacy Directive)		
Directive 2002/58/EC is amended as follows:		
1. Article 4 is deleted;	~~1. Article 4 is deleted;~~	CZ: This article constitutes a sectoral lex specialis to Article 32 of the GDPR and is crucial for protecting the confidentiality of electronic communications transmissions, including aspects not covered by the GDPR, for example network integrity, security of communications, mandatory incident reporting. The GDPR regulates the protection of personal data, not the confidentiality of the communication itself or the integrity of the transmission. Nor can it regulate them, otherwise it would not be technologically neutral.
2. After Article 5(3), the following subparagraph is added:		
'This paragraph shall not apply if the subscriber or user is a natural person, and the information stored		

Commission proposal	Drafting suggestions	Comments
or accessed constitutes or leads to the processing of personal data.'		
[…]		
Article 10		
Repeals and transitory clauses		
1. Regulation 2019/1150/EU is repealed with effect from [date = entry into application of this Regulation].		
2. By way of derogation from paragraph 1, the following provisions shall continue to apply until 31 December 2032:	2. By way of derogation from paragraph 1, the following provisions shall continue to apply until 31 December 2032**, or until date set out in relevant prospective amendment to the Regulation (EU) 2022/2065, whichever shall occur first:**	CZ: CZ considers that it would be appropriate to set an alternative end of application of the Regulation 2019/1150/EU (hereinafter referred to as "the P2B Regulation"), namely on the date of the report with the attached proposal for amendment pursuant to Article 91(2) and (3) of Regulation (EU) 2022/2065 (hereinafter referred to as "the DSA Regulation"). P2B Regulation contains some positive legal instruments that the Commission may consider transposing into the DSA Regulation even before 31 December 2032, and therefore, if the Commission proposes an amendment to the

Commission proposal	Drafting suggestions	Comments
		DSA Regulation before that date, it is reasonable for the P2B Regulation to be repealed at that earlier date. CZ**: CZ supports the idea of withdrawing some parts of the P2B to lower regulatory burden.** Nevertheless, we would like to emphasize once again that we have doubts as to whether P2B is fully replaced by other regulations such as DSA and DMA. The regulations pursue different objectives and protect different groups of entities. The P2B is stricter in certain respects and sets a higher standard of protection (e.g., the obligation to provide information about changes to terms and conditions or the obligation to provide rankings for all online intermediary services.).
	Article 1	CZ: Article 1 of the P2B Regulation establishes the personal and territorial scope of the P2B Regulation, together with the relationship to other Union law and national rules. The determination of the scope of a legal norm is a fundamental prerequisite for its validity, and it is therefore crucial that Article 1 of the P2B Regulation is retained, as otherwise it would not be possible to enforce the obligations under the P2B Regulation at all. (Possibly legal service could take an opinon to this.)
(a) Article 2, point (1);		
(b) Article 2, point (2);		

Commission proposal	Drafting suggestions	Comments
	Article 2, point (3);	CZ (to Art. 2(3)) The definition of a provider of online intermediation services is essential for interpreting the provisions retained in the P2B Regulation. This includes Articles 4 and 11 of the P2B Regulation that are to be retained under Commision proposal. Repealing the definition would create unnecessary legal uncertainty, and it is therefore proposed that Article 2, point (3) of the P2B Regulation is retained.
	Article 2, point (4);	CZ (to Art. 2(4)) The term "consumer" is included in the obligations that CZ proposes to retain (e.g., Article 3(4), point (b) of the P2B Regulation), but also in the definition of a business user. Repealing the definition would create unnecessary legal uncertainty, and it is therefore proposed that Article 2, point (4) of the P2B Regulation is retained.
(c) Article 2, point (5);		CZ (to Art. 2(5)) The term “online search engine” is included in the definition of the term “provider of online search engines”. The term “provider of online search engines” is included in obligations that CZ proposes to retain (e.g., Article 5(2) of the P2B Regulation). If the obligations proposed by CZ are retained, the repeal of the definition would create unnecessary legal uncertainty, and it is therefore proposed that Article 2, point (5) of the P2B Regulation is retained.
	Article 2, point (6);	CZ (to Art. 2 (6)) The term “provider of online search engines” is included in obligations that CZ proposes to retain (e.g., Article 5(2) of the P2B

Commission proposal	Drafting suggestions	Comments
		Regulation). If the obligations proposed by CZ are retained, the repeal of the definition would create unnecessary legal uncertainty, and it is therefore proposed that Article 2, point (6) of the P2B Regulation is retained.
	Article 2, point (7);	CZ (to Art. 2 (7)) The term "corporate website user" is included in obligations that CZ proposes to retain (e.g. Article 5(3) of the P2B Regulation). If the obligations proposed by CZ are retained, the repeal of the definition would create unnecessary legal uncertainty, and it is therefore proposed that Article 2, point (7) of the P2B Regulation is retained.
	Article 2, point (8);	CZ (to Art. 2 (8)) The term "ranking" is included in obligations that CZ proposes to retain (e.g. Article 5(2) of the P2B Regulation). If the obligations proposed by CZ are retained, the repeal of the definition would create unnecessary legal uncertainty, and it is therefore proposed that Article 2, point (8) of the P2B Regulation is retained.
	Article 2, point (10);	CZ (to Art. 2 (10)) The term "terms and conditions" is included in obligations that CZ proposes to retain (e.g. Article 3(1), point (b) of the P2B Regulation) and even in obligations that Comission proposes to retain (e.g. Article 11 of the P2B Regulation). Repealing the definition would create unnecessary legal uncertainty, and it is

Commission proposal	Drafting suggestions	Comments
		therefore proposed that Article 2, point (10) of the P2B Regulation is retained.
	Article 2, point (13);	CZ: The term "durable medium" is included in obligations that Comission proposes to retain (e.g. Article 4 of the P2B Regulation). Repealing the definition would create unnecessary legal uncertainty, and it is therefore proposed that Article 2, point (13) of the P2B Regulation is retained.
	Article 3(1), point (b);	CZ (to Art. 3 (1)(b)) proposes that the obligation of providers of online intermediation services to ensure that their terms and conditions are easily available to business users, including in the pre-contractual stage, is retained. Compared to Article 14(1) of the DSA Regulation, this obligation applies both to the pre-contractual stage and to a wider range of information. This requirement is on its own essential for the purposes of transparency and the principle of good faith, e.g. with regard to access to data (which shall be repealed by the Commission's proposal but generally permitted in accordance with the principle of contractual freedom).
	Article 3, point (2) ; **Article 3, point (4);**	CZ (to Art. 3(2);(4)) CZ proposes that the obligations of providers of online intermediary service regarding changes to their terms and conditions, shall be retained.

Commission proposal	Drafting suggestions	Comments
	Article 3, point (3)	Protecting business users from arbitrary changes to terms and conditions is essential, this is apparent also from the fact, that Commission plans to not repeal Article 4 of the P2B Regulation. Otherwise, business users would not be directly informed of the changes in terms and conditions, which would have an adverse effect on their provision of goods and services through the provider's service. If we repeal obligation to inform users about changes in their terms and conditions in advance, platforms could utilize changing of their terms and conditions for the purpose of restriction, suspension or termination of user accounts, which is something what Article 4 of the P2B Regulation strives to prevent. However, it is also appropriate to retain the exemptions from this obligation under Article 3(4) of the P2B Regulation and to allow providers of online intermediation service to change their terms and conditions rapidly in exceptional circumstances. CZ: (to Art. 3(3)) proposes to retain principle of absolute invalidity for both Article 3(1)(b) and Article 3(2) of the P2B Regulation. The invalidity of terms and conditions or their changes is an important private law instrument that business users can use to protect themselves against violations of the P2B Regulation by online intermediary service providers.

Commission proposal	Drafting suggestions	Comments
(d) Article 4;		
	Article 5, point (2) ; **Article 5, point (4) ;**	CZ: (to Art. 5(2); 5(4)) CZ proposes that the obligations of providers of online search engines in relation to ranking according to Article 5(2) to (6) of the P2B Regulation, are retained. Paragraphs (3), (5) and (6) need to be amended due to deletion of paragraph (1). Therefore these are mentioned bellow in new paragraph 3. These obligations are set out exclusively in the P2B Regulation and do not overlap with, for example, Article 27 of the DSA Regulation, because this provision of the DSA Regulation applies only to "mid-size" providers of online platforms, **not providers of online search engines**. Online search engines serve as gateways to information available on the internet, and therefore the repeal of these obligations may have an indirect impact on human rights of bussiness users such as freedom of expression or free enterprise.
	Article 8, point (b) ;	CZ: (to Art. 8 (b)) CZ proposes that the obligation of provider of online intermediation services to include information on the conditions under which business users can terminate the contractual relationship with the provider to their terms and conditions, is retained.

Commission proposal	Drafting suggestions	Comments
		It is very important that business users are informed of the circumstances under which they may terminate the use of a service in the case of unilaterally determined terms and conditions. Otherwise, providers of online intermediation services may, contrary to the principle of good faith, completely omit the option for business users to terminate the service and not allow them to do so. Or they could charge users with additional costs or fines. While this practice could be, in theory, dealt with through the civil proceedings, considering the will of small business users to engage in lenghty proceedings, public oversight should be considered as quite useful in this case. It is also important to note that this obligation is not explicitly laid down in any other Union legislation, as, for example, Article 14(1) of the DSA Regulation only applies to grounds for restricting services by providers of online intermediation services.
(e) Article 11;	**(e) Article 11, point (1), (2), (3) and (5);**	CZ welcomes the proposal to retain Article 11 of the P2B Regulation, but proposes the repeal of Article 11(4) of the P2B Regulation. Supervisory practice in Czech Republic has shown that the obligation to establish information on the functioning and effectiveness of the internal complaint-handling system does not bring any significant benefits to business users or the general public, thereby creating an unnecessary time,

Commission proposal	Drafting suggestions	Comments
		administrative, and financial burden for providers of online intermediation services. CZ also points out that a similar obligation is already laid down in Article 15(1), point (d) of the DSA Regulation, and therefore the retention of Article 11(4) of the P2B Regulation appears to be redundant. We would like to ask the Commission to explain why Article 11 of P2B needs to be maintained and how it is linked to the Platform Workers Directive.
(f) Article 15.		
	<u>Article 19</u> **<u>Article 10 [3] (of digital omnibus)</u>** **<u>3. By way of derogation from paragraph 1, the following provisions shall continue to apply until 31 December 2032 and shall be amended as follows:</u>** **<u>1. Article 5(3) is replaced by the following:</u>**	CZ: Article 19 of the P2B Regulation establishes the temporal scope of application of the P2B Regulation. That is one of the essential requirements for the validity of a legal norm, and therefore it is necessary to consider whether it is possible to repeal the provision without replacing it in adequate manner. **CZ: Art. 10(3) Digital Omnibus** We propose to create a new article of the digital omnibus regulation. Those proposed amendments to Article 5 of the P2B Regulation are necessary in order to avoid references to Article 5(1) of the P2B Regulation, which is to be repealed, thereby preventing legal uncertainty. Otherwise, the

Commission proposal	Drafting suggestions	Comments
	‘3. Where the main parameters include the possibility to influence ranking against any direct or indirect remuneration paid by business users or corporate website users to the respective provider, that provider shall also set out a description of those possibilities and of the effects of such remuneration on ranking in accordance with the requirements set out in paragraph 2 **2. Article 5(5) is replaced by the following:** **‘5. The descriptions referred to in paragraphs 2 and 3 shall be sufficient to enable the business users or corporate website users to obtain an adequate understanding of whether, and if so how and to what extent, the ranking mechanism takes account of the following:** **(a) the characteristics of the goods and services offered to consumers through the online search engine;** **(b) the relevance of those characteristics for those consumers;** **(c) the design characteristics of the website used by corporate website users.** **3. Article 5(6) is replaced by the following:**	provisions of Article 5(2) to (6) of the P2B Regulation would refer to legal obligations that have already been repealed. We propose these changes to exempt online intermediaries from the obligations regarding the search functionalities from the P2B, however, we would like to keep these obligation for search engines, as those are not covered by DSA or DMA.

Commission proposal	Drafting suggestions	Comments
	‘6. Providers of online search engines shall, when complying with the requirements of this Article, not be required to disclose algorithms or any information that, with reasonable certainty, would result in the enabling of deception of consumers or consumer harm through the manipulation of search results. This Article shall be without prejudice to Directive (EU) 2016/943.	
3. The following acts are repealed, with effect from [Date, aligned with the entry into application of the amendments]:		
a) Regulation (EU) 2022/868;		
b) Regulation (EU) 2018/1807;		
c) Directive 2019/1024.		
4. References to Regulation (EU) 2022/868, Regulation (EU) 2018/1807 and Directive 2019/1024 shall be read in accordance with the correlation table set out in Annex I of this Regulation.		

Commission proposal	Drafting suggestions	Comments
Article 11		
Final provisions		
This Regulation shall enter into force on the third day following that of its publication in the *Official Journal of the European Union*.		
Deviating from paragraph 3, Article 5(2) shall enter into application 6 months after the publication in the Official Journal of the European Union.		
Article 3(8), points (a) to (c), Articles 6 (2) and (3) and 7 to 9, shall enter into application 18 months from the entry into force of this Regulation. Deviating from the first sentence, where the Commission finds in its assessment pursuant to Article 23a (7) of Directive (EU) 2022/2555 that the single-entry point does not ensure the proper functioning, reliability, integrity or confidentiality, the obligations to report via the single-entry point set out in Article 23(4) of Directive (EU) 2022/2555, Article 19a (1a), Article 24 (2a) and Article 45a (3a) of Regulation (EU) 910/2014, Article 33 (1) of Regulation (EU) 2016/679, Article 19 (1) and (2) of Regulation (EU)	Article 3(8), points (a) to (c), Articles 6 (2) and (3) and 7 to 9, shall enter into application ~~18~~ **30** months from the entry into force of this Regulation. Deviating from the first sentence, where the Commission finds in its assessment pursuant to Article 23a (7) of Directive (EU) 2022/2555 that the single-entry point does not ensure the proper functioning, reliability, integrity or confidentiality, the obligations to report via the single-entry point set out in Article 23(4) of Directive (EU) 2022/2555, Article 19a (1a), Article 24 (2a) and Article 45a (3a) of Regulation (EU) 910/2014, Article 33 (1) of Regulation (EU) 2016/679, Article 19 (1) and (2) of Regulation (EU) 2022/2554, and Article 15(1) of Directive (EU)	CZ: The standard period for adapting is insufficient, based on the experience of member states' legislation. An extension to 30 months is likely to provide greater legal certainity.

Commission proposal	Drafting suggestions	Comments
2022/2554, and Article 15(1) of Directive (EU) 2022/2557 shall enter into application 24 months from the entry into force of this Regulation.	2022/2557 shall enter into application ~~24~~ **30** months from the entry into force of this Regulation	
This Regulation shall be binding in its entirety and directly applicable in all Member States.		
Done at Brussels,		
For the European Parliament *For the Council*		
The President *The President*		