Council of the European Union
General Secretariat

Interinstitutional files:
2025/0360 (COD)

Brussels, 30 March 2026

WK 3736/2026 ADD 4

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:	Consultation on Omnibus VII (GDPR/P2B/ePrivacy) Digital rules - related to AGS meeting of 27.02.26 (deadline 18.03.26) - consolidated written comments on GDPR/P2B & ePrivacy files - FR, PL and RO comments on GDPR/P2B

Delegations will find attached addtional comments on GDPR/P2B submitted by France, Poland and Romania.

Digital omnibus on GDPR/P2B Deadline: ***18 March 2026***
From: FR, PL, RO **Updated: 30/03/2026 12:00**

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!

Presidency compromise text	Drafting suggestions and Comments
General Comments	
REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854, (EU) 2022/2554, and (EU) 910/2014 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) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus)	
(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~~	FR (Comments):

Presidency compromise text	Drafting suggestions and 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 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[1]. 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.~~	La France salue la modification apportée par la Présidence, qui permet de conserver la définition actuelle de donnée personnelle, telle qu'interprétée par la CJUE dans sa jurisprudence la plus récente. PL (Drafting suggestions): We welcome the deletion of the proposed changes to the definition of personal data in recital 27, but remain open to find a solution addressing the topic without changing the definition.

Presidency compromise text	Drafting suggestions and Comments
1 ~~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)~~	
(27a) 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, it is important to provide further clarity on when a natural person should be considered to be identifiable. The European Data Protection Board should support controllers by adopting guidelines assessing and specifying the state of the art of available techniques, as well as the technical and organisational measures and criteria to pseudonymise personal data effectively, and clarifying circumstances whether a natural person is identifiable and means reasonably likely to be used to identify a natural person, including means and criteria to determine whether data resulting from pseudonymisation may no longer constitute personal data for certain entities. While controllers remain fully responsible to determine whether data resulting from pseudonymisation is personal, the guidelines should support controllers in implementing such measures and criteria, and provide guidance to demonstrate whether pseudonymised data do not lead to re-identification of data subjects.	FR (Drafting suggestions): (27a) 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, it is important to provide further clarity on when a natural person should be considered to be identifiable. The European Data Protection Board should support controllers by adopting ~~guidelines~~ **an opinion** assessing and specifying the state of the art of available techniques, as well as the technical and organisational measures and criteria to pseudonymise personal data effectively, and clarifying circumstances whether a natural person is identifiable and means reasonably likely to be used to identify a natural person, including means and criteria to determine whether data resulting from pseudonymisation may no longer constitute personal data for certain entities. While controllers remain fully responsible to determine whether data resulting from pseudonymisation is personal, the guidelines should support controllers in implementing such measures and criteria, and provide guidance to demonstrate whether pseudonymised data do not lead to re-identification of data subjects. FR (Comments):

Presidency compromise text	Drafting suggestions and Comments
	Les autorités françaises proposent qu'en lieu et place de lignes directrices, le CEPD adopte un avis, qui pourrait ainsi être rendu contraignant. Des propositions infra sur les articles vont aussi dans ce sens. PL (Drafting suggestions): The wording referring to "criteria to determine whether data resulting from pseudonymisation may no longer constitute personal data for certain entities" may create uncertainty as regards the definition of personal data under Article 4(1) of Regulation (EU) 2016/679 and should therefore be clarified. Possible drafting clarification: "…including means and criteria to assess the risk of re-identification and the effectiveness of pseudonymisation techniques, without affecting the definition of personal data set out in Article 4(1) of Regulation (EU) 2016/679." PL (Comments): The current wording could be interpreted as suggesting that pseudonymised data may cease to constitute personal data for certain entities. This could create uncertainty regarding the scope of the definition of personal data under Article 4(1) GDPR and its interpretation. Clarification would therefore be welcome to ensure that this recital does not alter the existing legal framework, under which pseudonymised data generally remain personal data. We nevertheless recognise the importance of providing additional clarity regarding pseudonymisation and the role of the European Data Protection Board in supporting controllers through guidance. RO (Drafting suggestions):

Presidency compromise text	Drafting suggestions and Comments
	Guidelines should be proportionate and include simplified compliance pathways for SMEs." RO (Comments): We support the introduction of additional criteria on the identifiability of the person, in particular by referring to the "means reasonably likely to be used" by the controller, as this reduces legal uncertainty for SMEs. SMEs do not have the technical capacity for complex assessments on re-identification.
~~(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 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).~~	PL (Drafting suggestions): The deletion of recital 28 may remove useful interpretative elements clarifying the notion of scientific research for the purposes of Regulation (EU) 2016/679 and should therefore be reconsidered. PL (Comments): The removal of this recital may reduce legal clarity regarding the notion of scientific research and its relationship with the principle of purpose limitation. Further work may therefore be needed to ensure a common understanding of the concept of scientific research under the GDPR. We remain open to finding a balanced compromise in this area.
(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~~**should not be** necessary to ascertain on the basis of Article 6(4) of ~~this~~ Regulation **(EU) 2016/679** whether the purpose of the further processing is compatible with the purpose for which the personal data are initially collected. **Such further processing should be**	FR (Drafting suggestions): (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 should not be necessary to ascertain on the basis

Presidency compromise text	Drafting suggestions and Comments
considered compatible, provided that it is carried out in compliance with the principle of purpose limitation and subject to appropriate safeguards laid down in Regulation (EU) 2016/679, in particular Article 89. The qualification of processing as being carried out for scientific research purposes should be based on objective characteristics of the research activity and should not rely solely on the declaration of the controller, nor undermine the obligation to apply appropriate safeguards as provided for in Article 89 of Regulation (EU) 2016/679. In order to assess whether scientific research activities meet the conditions of scientific research for the purpose of Regulation (EU) 2016/679, account can be taken of elements such as the purpose of the research, the methodological approach and ethical standards applied in the specific area while conducting the research, and adherence to the principles of transparency, reliability, accountability and oversight, verifiability, and rules for research integrity. Scientific research activities should concur to public interest and well-being, prevent individuals from being subjected to harm or other adverse effects due to participating in scientific research and include – among other things – the respect for human autonomy and the notion of consent to participate in research. Scientific research activities can, amongst others, support innovation such as technology development and may be conducted in academic, industry and other settings, by public authorities or private entities, including small and medium sized undertakings.	of Article 6(4) of Regulation (EU) 2016/679 whether the purpose of the further processing is compatible with the purpose for which the personal data are initially collected. Such further processing should be considered compatible, provided that it is carried out in compliance with the principle of purpose limitation and subject to appropriate safeguards laid down in Regulation (EU) 2016/679, in particular Article 89. The qualification of processing as being carried out for scientific research purposes should be based on objective characteristics of the research activity and should not rely solely on the declaration of the controller, nor undermine the obligation to apply appropriate safeguards as provided for in Article 89 of Regulation (EU) 2016/679. In order to assess whether scientific research activities meet the conditions of scientific research for the purpose of Regulation (EU) 2016/679, account **should** ~~can~~ be taken of elements such as the purpose of the research, the methodological approach and ethical standards applied in the specific area while conducting the research, and adherence to the principles of transparency, reliability, accountability and oversight, verifiability, and rules for research integrity. Scientific research activities should **be conducted autonomously and independently, free from undue pressure and** concur to public interest and well-being, prevent individuals from being subjected to harm or other adverse effects due to participating in scientific research and include – among other things – the respect for human autonomy and the notion of consent to participate in research. Scientific research activities can, amongst others, support innovation such as technology development and may be conducted in academic, industry and other settings, by public authorities or private entities, including small and medium sized undertakings. FR (Comments):

Presidency compromise text	Drafting suggestions and Comments
	La France souhaite préciser des garde-fous relatifs à l'indépendance de la recherche. PL (Drafting suggestions): The wording referring to objective characteristics of scientific research and to elements such as ethical standards, transparency and research integrity may require further clarification to ensure legal certainty regarding the notion of scientific research under Regulation (EU) 2016/679. Consider streamlining the recital so that it focuses on the compatibility of further processing for research purposes. PL (Comments): The expanded wording introduces several elements that could be interpreted as additional criteria for qualifying processing as scientific research. This may create uncertainty regarding the interpretation of the notion of scientific research and its interaction with the principle of purpose limitation. Clarification of the recital may therefore be useful to ensure legal certainty and a balanced approach to further processing for research purposes. RO (Drafting suggestions): „…including innovation activities carried out by SMEs, such as product development and applied research.”

Presidency compromise text	Drafting suggestions and Comments

Presidency compromise text	Drafting suggestions and Comments
	RO (Comments): This ensures that SMEs have real access to the research-friendly regime.

Presidency compromise text	Drafting suggestions and Comments
(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 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.	PL (Drafting suggestions): Previous comments remain valid.
(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	PL (Drafting suggestions):

Presidency compromise text	Drafting suggestions and Comments
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, 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.	Previous comments remain valid. RO (Drafting suggestions):

Presidency compromise text	Drafting suggestions and Comments
	We propose to eliminate or to clarify the concept of ”*regurgitation*”. RO (Comments):

Presidency compromise text	Drafting suggestions and Comments
	There is no definition to clarify the significance of this term and it is not used within the provisions of the draft regulation.
(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~~**may be necessary for the purposes of the** legitimate ~~interest~~**interests pursued by a controller or by a third-party** 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. Scientific research can also follow public interest and be based on Member States and Union** 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) 2016/679 as well as all other requirements and principles of that Regulation are met.	PL (Drafting suggestions): Poland notes the minor modification of Recital (32). Our previous comments remain valid.
(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	FR (Drafting suggestions): (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

Presidency compromise text	Drafting suggestions and Comments
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 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.	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, **or would be technically impossible,** the controller should effectively protect such data 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. FR (Comments): Les autorités françaises souhaitent que la rédaction soit alignée sur d'autres dispositions du RGPD qui mentionnent l'effort disproportionné ou l'impossibilité technique, ce afin que le seuil soit le même. PL (Drafting suggestions): Previous comments remain valid. RO (Drafting suggestions):

Presidency compromise text	Drafting suggestions and Comments
	„…taking into account the size, resources and capabilities of the controller, in particular SMEs." RO (Comments): The technical requirements for removing sensitive data may be excessive for SMEs.
(34) **Processing of** 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 **(EU) 2016/679** should ~~also~~ be allowed where the verification of the claimed identity of the data subject is necessary **and proportionate** for a purpose pursued by the controller~~,~~ and **when provided for under Union or Member States law. The controller should choose from equally effective means the less intrusive one. This derogation should apply where** suitable safeguards apply to ~~enable the data subject to have sole control of~~**ensure that the biometric data or the means needed for** the verification ~~process~~**are under the sole control and possession of the data subject**. For example, **this is the case** where the biometric data are securely stored solely at the ~~side~~**device** of the data subject or are securely stored ~~at the side of~~**by** the controller in a state-of-the-art encrypted form and the encryption key or equivalent means is **securely** held solely by the data subject, ~~that~~**and subject to measures**	FR (Comments): Les autorités françaises sont tout à fait favorables aux amendements introduits. Ceux-ci permettent de mieux encadrer cette nouvelle base légale pour le traitement de données particulièrement sensibles. Dans ce contexte, elles estiment qu'il est disproportionné de prévoir que ces données pourront être traitées au seul motif qu'un responsable de traitement estime que la reconnaissance biométrique serait utile. Comme pour de nombreuses autres dispositions à l'article 9, paragraphe 2, les autorités françaises estiment qu'il est au contraire nécessaire de n'autoriser le traitement des données biométriques pour l'identification des personnes concernées que lorsque la loi de l'Etat membre ou de l'Union le prévoit. En effet, sans cette garantie supplémentaire, la modification du RGPD aboutirait à consacrer en droit de l'Union le droit pour tout responsable de traitement d'imposer la reconnaissance biométrique sans autre motif que celui de la disponibilité de la technologie. Les autorités françaises estiment que si cette reconnaissance peut être utile dans certains cas, notamment pour tenir compte d'obligations de l'employeur en matière de sécurité, le recours à ce type de technologie doit refléter la volonté du législateur d'avoir recours à une technologie très intrusive dans chaque secteur ou situation spécifique et que le choix d'ouvrir cette possibilité dans tout domaine ne relève pas du RGPD. Les autorités françaises estiment que la modification du RGPD doit conduire à s'assurer

Presidency compromise text	Drafting suggestions and Comments
ensuring the overall security of processing ~~is not likely to create significant risks to his or her fundamental rights and freedoms. The controller does not gain knowledge of the~~**, including during the enrolment phase of data subject's** biometric data ~~or only for a very limited time~~**and** during the verification process.	que ce cadre juridique ne sera pas bloquant en la matière, mais qu'il ne doit pas à aboutir à opérer un choix politique qui ne relève pas de la protection des données, de généraliser la reconnaissance biométrique en confiant aux responsables de traitement le choix d'avoir recours ou non à ce type de technologie. PL (Drafting suggestions): Clarify that the derogation from Article 9(1) GDPR for biometric verification must be interpreted restrictively and applied only where the processing is necessary, proportionate and subject to appropriate safeguards ensuring that the data subject retains effective control over the verification process. PL (Comments): Poland notes that the revised wording introduces additional safeguards, including the requirement of necessity, proportionality and a legal basis in Union or Member State law. These elements go into the right direction. However, given the particularly sensitive nature of biometric data, it remains important to ensure that the derogation from Article 9 GDPR is interpreted narrowly and consistently across Member States.
(35) Article 15 of Regulation (EU) 2016/679 provides data subjects with the right to obtain **confirmation** 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 **(5) of that** ~~of the~~ Regulation **already provides that where the request to exercise** ~~that~~ the right of access~~, which is~~	FR (Drafting suggestions): (35) Article 15 of Regulation (EU) 2016/679 provides data subjects with the right to obtain confirmation from the controller 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

Presidency compromise text	Drafting suggestions and Comments
~~from the outset favourable to data subjects,~~ **is manifestly unfounded or excessive, the controller may either charge a reasonable fee or refuse to act on the request. It is important to clarify that this** should ~~not be abused in the sense that~~**apply also where an abusive intention on the part of** the data ~~subjects abuse them for purposes other than the protection of their data~~**subject submitting those requests can be demonstrated by the controller**. For example, such an ~~abuse of the right of access~~**abusive intention** would arise where the data subject ~~intends to cause the controller to refuse an access request, in order to subsequently demand the payment of compensation, potentially under the threat of bringing a claim for damages. Other examples of abuse include situations where data subjects make~~**submits** excessive ~~use of the right of access~~**numbers of identical or largely similar requests** with the ~~only~~**sole** intent of causing damage or harm to the controller**. Another example of abusive intention includes situations** ~~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.~~	other rights under Regulation (EU) 2016/679. Article 12 (5) of that Regulation already provides that where the request to exercise the right of access ~~is~~ manifestly unfounded or excessive, the controller may either charge a reasonable fee or refuse to act on the request. It is important to clarify that this should apply also where an abusive intention on the part of the data ~~s~~subject submitting those requests can be demonstrated by the controller. For example, such an abusive intention would arise where the data subject submits excessive numbers of identical or largely similar requests with the sole intent of causing damage or harm to the controller. Another example of abusive intention includes situations ~~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 **or when the exercise of this would adversely affect judicial procedures**. FR (Comments): Les autorités françaises souhaitent qu'il soit également prévu le cas où l'exercice du droit d'accès affecterait négativement une procédure qui prévoit déjà elle-même des règles d'accès aux informations dans ce contexte afin d'éviter aussi les contournements de procédures. PL (Drafting suggestions): Clarify that the notion of "abusive intention" and the assessment of whether a request is excessive or abusive should be interpreted restrictively and in accordance with the principle of proportionality, so as not to undermine the essence of the right of access under Article 15 of Regulation (EU) 2016/679. PL (Comments):

Presidency compromise text	Drafting suggestions and Comments
	Poland notes that the revised wording of Recital (35) clarifies the circumstances in which controllers may consider requests for access abusive, in particular by referring to demonstrable abusive intention. This clarification goes into the right direction and helps address situations involving clearly instrumental use of the right of access.
(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 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~~**that** 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~~**that** 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 **of Article 13** 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. **The application of the derogation from the information obligation should not undermine the principle of transparency and should be limited to situations where the controller can objectively demonstrate that the data subject already possesses the required information.** These should be the situations where the **personal data are collected in the** context of ~~the~~**a direct, limited and clearly circumscribed** relationship between ~~the~~**data subjects and a** controller and ~~the data subject is very clear and circumscribed and the controller's activity is not data-intensive~~**does not involve the processing of a large amount of personal data**, such as the relationship between a craftsman and their clients, where	PL (Comments): Poland welcomes the revised wording of Recital (36) This clarification addresses the concerns previously raised regarding the potentially broad interpretation of concepts such as "non data-intensive processing" or limited processing contexts and contributes to ensuring a proportionate and consistent application of the GDPR.

Presidency compromise text	Drafting suggestions and Comments
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 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 **further** processing **by the same controller** 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 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	PL (Drafting suggestions): Previous drafting suggestion remains valid. PL (Comments):

Presidency compromise text	Drafting suggestions and Comments
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.	Poland notes the clarification introduced in Recital (37) referring to further processing by the same controller. However, the concerns previously raised regarding the exceptional nature of the derogation from the information obligation and the need for a case-by-case assessment remain valid.
~~(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 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.~~	PL (Drafting suggestions): Poland does not support the deletion of Recital (38). The issue of automated decision-making under Article 22 GDPR requires further clarification in order to ensure legal certainty while safeguarding the rights of data subjects. PL (Comments): In light of the increasing use of automated and AI-based systems, further clarification of art. 22 remains important. Poland considers that the recital should not lead to an expansion of fully automated decision-making beyond the conditions already established in the GDPR. In particular, the requirement of necessity under Article 22(2)(a) GDPR should be interpreted restrictively and the use of automated decision-making should remain proportionate and appropriately assessed with regard to its impact on the rights and freedoms of natural persons. For these reasons, the issue addressed in Recital (38) should be further refined rather than removed from the text.

Presidency compromise text	Drafting suggestions and Comments
(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 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~~**establish and make public** 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~~**, as well as a common list of circumstances in which a personal data breach does not result in such a high risk**. 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. **The alignment of notification thresholds does not affect the controller's obligation to carry out an individual risk assessment and to maintain complete documentation of personal data breaches in accordance with Article 33(5) and Article 30 of Regulation (EU) 2016/679.**	FR (Drafting suggestions): (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. FR (Comments): Les premières phrases sont explicatives de la modification apportées au RGPD mais ne sont pas celles d'un considérant. PL (Comments): Poland supports the revised wording

Presidency compromise text	Drafting suggestions and Comments
(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 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~~**established and made public** by the Board ~~and adopted by the Commission as an implementing act~~. In order to facilitate compliance by controllers, the Board should also ~~prepare~~**establish and make public** 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 be reviewed at least every three years and updated where necessary.	PL (Drafting suggestions): Add at the end: “When applying those lists, due account should be taken of the context, nature, scope and purposes of the specific processing operations, in accordance with the risk-based approach underpinning Regulation (EU) 2016/679.” PL (Comments): The current wording of Recital (40) does not sufficiently reflect the risk-based approach underpinning the GDPR. When applying EU-level lists of processing operations requiring a DPIA, it remains necessary to take into account the context, nature, scope and purposes of the specific processing operations. Without such clarification, there is a risk that the lists could be interpreted too rigidly, potentially limiting the flexibility needed for the practical application of Article 35 GDPR.

Presidency compromise text	Drafting suggestions and Comments
(41) Regulation (EU) 2018/1725 of the European Parliament and of the Council[2] 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[3] 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. 2 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). 3 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 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).	FR (Drafting suggestions): ~~(41) Regulation (EU) 2018/1725 of the European Parliament and of the Council[2] 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[3] 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.~~ FR (Comments): L'alignement de ces textes ne peut pas être prévu par un considérant. PL (Drafting suggestions): Previous comments remain valid.
(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	FR (Drafting suggestions): ~~(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,~~

Presidency compromise text	Drafting suggestions and Comments
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.	~~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.~~ FR (Comments): L'alignement de ces textes ne peut pas être prévu par un considérant.
(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 into application of the amendments to Regulation (EU) 2016/679 and Regulation (EU) 2018/1725.	FR (Drafting suggestions): ~~(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 into application of the amendments to Regulation (EU) 2016/679 and Regulation (EU) 2018/1725.~~ FR (Comments): L'alignement de ces textes ne peut pas être prévu par un considérant. PL (Comments): Previous comments remain valid.

Presidency compromise text	Drafting suggestions and Comments
(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.	FR (Drafting suggestions): ~~(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.~~ FR (Comments): Les autorités françaises attirent l'attention de la Présidence sur les commentaires sur la proposition de nouvel article 88a : la directive ePrivacy concerne des opérations techniques de dépôt de cookies qui ne s'apparentent pas à des traitements de données. Assimiler le fondement du dépôt de cookie à un traitement apparaît inopportun, et inadapté en termes d'assimilation de la base légale du traitement de données subséquent. En outre, cette intégration dans le RGPD laisse subsister un autre régime pour les données non personnelles. Les autorités françaises y sont également défavorables. PL

Presidency compromise text	Drafting suggestions and Comments
	(Drafting suggestions): Previous drafting suggestion remains valid. PL (Comments): Previous comments remain valid.
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 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.	FR (Drafting suggestions): ~~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 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.~~ FR (Comments): La directive ePrivacy concerne des opérations techniques de dépôt de cookies qui ne s'apparentent pas à des traitements de données. Assimiler le fondement du dépôt de cookie à un traitement apparaît inopportun, et inadapté en termes d'assimilation de la base légale du traitement de données subséquent. En outre, cette intégration dans le RGPD laisse subsister un autre régime pour les données non personnelles. Les autorités françaises y sont également défavorables.

Presidency compromise text	Drafting suggestions and Comments
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.	FR (Drafting suggestions): ~~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.~~ FR (Comments): La directive ePrivacy concerne des opérations techniques de dépôt de cookies qui ne s'apparentent pas à des traitements de données. Assimiler le fondement du dépôt de cookie à un traitement apparaît inopportun, et inadapté en termes d'assimilation de la base légale du traitement de données subséquent. En outre, cette intégration dans le RGPD laisse subsister un autre régime pour les données non personnelles. Les autorités françaises y sont également défavorables.
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	FR (Drafting suggestions): ~~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~~

Presidency compromise text	Drafting suggestions and Comments
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 should not give rise to the continuous monitoring of the data subject's private life.	~~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 should not give rise to the continuous monitoring of the data subject's private life.~~ FR (Comments): la directive ePrivacy concerne des opérations techniques de dépôt de cookies qui ne s'apparentent pas à des traitements de données. Assimiler le fondement du dépôt de cookie à un traitement apparaît inopportun, et inadapté en termes d'assimilation de la base légale du traitement de données subséquent. En outre, cette intégration dans le RGPD laisse subsister un autre régime pour les données non personnelles. Les autorités françaises y sont également défavorables.

Presidency compromise text	Drafting suggestions and Comments
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.	FR (Drafting suggestions): ~~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.~~ FR (Comments): La directive ePrivacy concerne des opérations techniques de dépôt de cookies qui ne s'apparentent pas à des traitements de données. Assimiler le fondement du dépôt de cookie à un traitement apparaît inopportun, et inadapté en termes d'assimilation de la base légale du traitement de données subséquent. En outre, cette intégration dans le RGPD laisse subsister un autre régime pour les données non personnelles. Les autorités françaises y sont également défavorables.
(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.	FR (Drafting suggestions): ~~(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.~~ FR

Presidency compromise text	Drafting suggestions and Comments
	(Comments): La directive ePrivacy concerne des opérations techniques de dépôt de cookies qui ne s'apparentent pas à des traitements de données. Assimiler le fondement du dépôt de cookie à un traitement apparaît inopportun, et inadapté en termes d'assimilation de la base légale du traitement de données subséquent. En outre, cette intégration dans le RGPD laisse subsister un autre régime pour les données non personnelles. Les autorités françaises y sont également défavorables. PL (Drafting suggestions): Previous drafting suggestion remains valid. PL (Comments): Previous comments remain valid.
(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 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	FR (Drafting suggestions): ~~(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 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~~

Presidency compromise text	Drafting suggestions and Comments
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.	~~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.~~ FR (Comments): La directive ePrivacy concerne des opérations techniques de dépôt de cookies qui ne s'apparentent pas à des traitements de données. Assimiler le fondement du dépôt de cookie à un traitement apparaît inopportun, et inadapté en termes d'assimilation de la base légale du traitement de données subséquent. En outre, cette intégration dans le RGPD laisse subsister un autre régime pour les données non personnelles. Les autorités françaises y sont également défavorables. PL (Drafting suggestions): Previous drafting suggestion remains valid. PL (Comments): Previous comments remain valid.
(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	FR (Drafting suggestions): ~~(47) Directive 2002/58/EC on privacy and electronic communications 'ePrivacy Directive'), last revised in 2009, provides a framework for the~~

Presidency compromise text	Drafting suggestions and Comments
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 constitute or lead to the processing of personal data.	~~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 constitute or lead to the processing of personal data.~~ FR (Comments): La directive ePrivacy concerne des opérations techniques de dépôt de cookies qui ne s'apparentent pas à des traitements de données. Assimiler le fondement du dépôt de cookie à un traitement apparaît inopportun, et inadapté en termes d'assimilation de la base légale du traitement de données subséquent. En outre, cette intégration dans le RGPD laisse subsister un autre régime pour les données non personnelles. Les autorités françaises y sont également défavorables.
(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	FR (Drafting suggestions): ~~(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~~

Presidency compromise text	Drafting suggestions and Comments
(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.	~~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.~~ FR (Comments): La directive ePrivacy concerne des opérations techniques de dépôt de cookies qui ne s'apparentent pas à des traitements de données. Assimiler le fondement du dépôt de cookie à un traitement apparaît inopportun, et inadapté en termes d'assimilation de la base légale du traitement de données subséquent. En outre, cette intégration dans le RGPD laisse subsister un autre régime pour les données non personnelles. Les autorités françaises y sont également défavorables.
(58) The European Data Protection Supervisor ~~was~~**and the European Data Protection Board were** consulted in accordance with Article ~~42(1)~~**42** of Regulation (EU) 2018/1725 of the European Parliament and of the Council[4], and delivered ~~its~~**their joint** opinion on ~~[DATE]. The European Data Protection Board was consulted in accordance with Article 42(2) of Regulation (EU) 2018/1725 and delivered an opinion on [DATE]~~**10 February 2026**. 4 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	

Presidency compromise text	Drafting suggestions and Comments
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).	
(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~~**2019/1150** 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 **and for purposes of keeping the necessary level of protection for business users**, 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, **or that are not covered by other legal acts,** in particular Directive (EU) 2023/2831 on improving working conditions in platform work, and Article 15 ensuring enforcement, will temporarily remain in application until ~~the original acts are amended.~~**2032.**	

Presidency compromise text	Drafting suggestions and Comments
(61) The amendments to Regulation (EU) 2016/679 and Regulation (EU) 2018/1725 are based on Article 16 TFEU. The amendments to Directive 2002/58/EC are based on Article 16 TFEU and Article 114 TFEU. All other amendments are based on Article 114 TFEU.	
Article 3 **Amendments to Regulation (EU) 2016/679 (GDPR)**	
Regulation (EU) 2016/679 is amended as follows:	
1. Article 4 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 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.'~~	FR (Comments): La France soutient cette suppression : pour maintenir la jurisprudence de la CJUE il convient de ne pas amender le texte qu'elle a déjà interprété, ce qui offre une sécurité juridique des acteurs. PL (Drafting suggestions): Poland welcomes the deletion of the proposed amendment to the definition of personal data. PL

Presidency compromise text	Drafting suggestions and Comments
	(Comments): The deletion preserves the existing interpretation of the concept of personal data under Regulation (EU) 2016/679 and avoids creating legal uncertainty. Poland remains open to find a solution addressing the challenge without changing the definition.
(b) the following points are added:	
'(32) 'terminal equipment' means terminal equipment as set out in Article 1(1) of Directive 2008/63/EC;	FR (Drafting suggestions): ~~'(32) 'terminal equipment' means terminal equipment as set out in Article 1(1) of Directive 2008/63/EC;~~ FR (Comments): La France rappelle sa position relative aux articles 88a et 88b Cette définition a vocation à intégrer les dispositions de la directive ePrivacy, ce qui n'est pas pertinent.
(33) for 'electronic communications networks' the definition of Article 2(1) of Directive (EU) 2018/1972 shall apply;	FR (Drafting suggestions): ~~(33) for 'electronic communications networks' the definition of Article 2(1) of Directive (EU) 2018/1972 shall apply;~~ FR (Comments): La France rappelle sa position relative aux articles 88a et 88b

Presidency compromise text	Drafting suggestions and Comments
	Cette définition a vocation à intégrer les dispositions de la directive ePrivacy, ce qui n'est pas pertinent.
(34) 'web browser' means web browser as defined in Article 2(11) of Regulation (EU) 2022/1925;	FR (Drafting suggestions): ~~(34) 'web browser' means web browser as defined in Article 2(11) of Regulation (EU) 2022/1925;~~ FR (Comments): La France rappelle sa position relative aux articles 88a et 88b Cette définition a vocation à intégrer les dispositions de la directive ePrivacy, ce qui n'est pas pertinent.
(35) 'media service' means a media service as defined in Article 2(1) of Regulation (EU) 2024/1083;	FR (Drafting suggestions): ~~(35) 'media service' means a media service as defined in Article 2(1) of Regulation (EU) 2024/1083;~~ FR (Comments): La France rappelle sa position relative aux articles 88a et 88b Cette définition a vocation à intégrer les dispositions de la directive ePrivacy, ce qui n'est pas pertinent.

Presidency compromise text	Drafting suggestions and Comments
(36) ‘media service provider’ means a media service provider as defined in Article 2(2) of Regulation (EU) 2024/1083;’	FR (Drafting suggestions): ~~(36) ‘media service provider’ means a media service provider as defined in Article 2(2) of Regulation (EU) 2024/1083;’~~ FR (Comments): La France rappelle sa position relative aux articles 88a et 88b Cette définition a vocation à intégrer les dispositions de la directive ePrivacy, ce qui n’est pas pertinent.
(37) ‘online interface’ means an online interface as defined in Article 3(m) of Regulation (EU) 2022/2065.’	FR (Drafting suggestions): ~~(37) ‘online interface’ means an online interface as defined in Article 3(m) of Regulation (EU) 2022/2065.’~~ FR (Comments): La France rappelle sa position relative aux articles 88a et 88b Cette définition a vocation à intégrer les dispositions de la directive ePrivacy, ce qui n’est pas pertinent.
~~(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~~	PL (Drafting suggestions):

Presidency compromise text	Drafting suggestions and Comments
~~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.'~~	The deletion of the definition of "scientific research" may reduce legal clarity and should be reconsidered. Further work on clarifying and appropriately limiting this concept would be preferable to its removal. PL (Comments): Clarifying the notion of "scientific research" could contribute to a more consistent application of the GDPR framework, in particular in relation to purpose limitation and the safeguards provided for in Article 89 GDPR. In particular, it should be ensured that the concept of scientific research is based on objective criteria and is not interpreted in a way that would allow processing carried out primarily for commercial product development to bypass the safeguards laid down in the GDPR.
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, **subject to the application of appropriate safeguards** 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** ('purpose limitation');'	PL (Drafting suggestions): Further processing for research, statistical or archiving purposes should remain clearly subject to the application of appropriate safeguards under Article 89(1) GDPR in order to preserve the principle of purpose limitation. PL (Comments): The revised wording partly addresses concerns previously raised regarding the need to ensure that further processing for scientific research, historical research or statistical purposes is subject to appropriate safeguards. However, considering that the compatibility test under Article 6(4) is no longer applicable in this context, it remains important to ensure that the

Presidency compromise text	Drafting suggestions and Comments
	principle of purpose limitation is not weakened and that the safeguards under Article 89(1) GDPR are applied in a meaningful and effective manner.
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.	FR (Comments): Les autorités françaises soutiennent l’avis du CEPD sur le fait qu’il conviendrait de préciser dans la rédaction du nouvel article 9(2)(k) qu’il vise le cas de traitement résiduel / incident de données de santé. En effet, pour développer un système d’IA dans le domaine de la santé, y compris un dispositif médical utilisant de l’IA, il faut pouvoir s’appuyer sur une autre exception de l’article 9§2 (par exemple 9§2a ou 9§2i) et il ne faudrait pas que l’exception 9§2k puisse être mal interprétée sur ce point. La rédaction actuelle du 9§2k « *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*. » pourrait laisser entendre qu’il s’agit de la seule exception mobilisable pour le traitement de données de santé dans le cadre du développement et de la mise en œuvre d’un système d’IA. PL (Drafting suggestions): Key concepts such as “residual presence of data” and “disproportionate effort” should be further clarified in order to ensure legal certainty and

Presidency compromise text	Drafting suggestions and Comments
	prevent an overly broad interpretation of the derogation from Article 9 GDPR. PL (Comments): Clarifying the distinction between incidental and intentional processing of special categories of data would help ensure that the derogation introduced for AI development does not unintentionally allow processing that deliberately relies on such data. Such clarification would contribute to legal certainty while preserving the pro-innovation objective of the provision and ensuring that the safeguards in Article 9(5) are applied effectively.
(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 **one-to-one** verification is under the sole control **and possession** of the data subject~~.~~ **and in so far as it is authorised by Union or Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject'**	FR (Comments): Les autorités françaises sont tout à fait favorables aux amendements introduits. Ceux-ci permettent de mieux encadrer cette nouvelle base légale pour le traitement de données particulièrement sensibles. Dans ce contexte, elles estiment qu'il est disproportionné de prévoir que ces données pourront être traitées au seul motif qu'un responsable de traitement estime que la reconnaissance biométrique serait utile. Ceci conduirait en outre à une plus grande fragmentation des pratiques que le renvoi à des garanties à prévoir en droit national qui existent déjà dans le cadre de l'article 9, en laissant la mise en place de ce type de traitement à la seule appréciation des responsables de traitements. Comme pour de nombreuses autres dispositions à l'article 9, paragraphe 2, les autorités françaises estiment ainsi qu'il est au contraire nécessaire de n'autoriser le traitement des données biométriques pour l'identification des personnes concernées que lorsque la loi de l'Etat membre ou de l'Union le prévoit. En effet, sans cette garantie supplémentaire, la modification du

Presidency compromise text	Drafting suggestions and Comments
	RGPD aboutirait à consacrer en droit de l'Union le droit pour tout responsable de traitement d'imposer la reconnaissance biométrique sans autre motif que celui de la disponibilité de la technologie. Les autorités françaises estiment que si cette reconnaissance peut être utile dans certains cas, notamment pour tenir compte d'obligations de l'employeur en matière de sécurité, le recours à ce type de technologie doit refléter la volonté du législateur d'avoir recours à une technologie très intrusive dans chaque secteur ou situation spécifique et que le choix d'ouvrir cette possibilité dans tout domaine ne relève pas du RGPD. A cet égard, les autorités françaises estiment que la confirmation de l'identité proposée ici ne se distingue en réalité pas d'une opération permettant d'identifier la personne de manière unique et qui est visée ici à l'article 9. Si ce qui est proposé ici, se distingue bien des traitements permettant l'identification d'une personne dans une foule, pour autant la confirmation de l'identité d'une personne reste un traitement de données sensibles nécessitant des garanties spécifiques et renforcées prévues dans le droit des Etats membres. Les autorités françaises estiment que la modification du RGPD doit conduire à s'assurer que ce cadre juridique ne sera pas bloquant en la matière, mais qu'il ne doit pas à aboutir à opérer un choix politique qui ne relève pas de la protection des données, de généraliser la reconnaissance biométrique en confiant aux responsables de traitement le choix d'avoir recours ou non à ce type de technologie. PL (Drafting suggestions): The interaction between the requirement of "sole control and possession of the data subject" and the condition that processing must be authorised by Union or Member State law should be clarified to ensure legal certainty. PL

Presidency compromise text	Drafting suggestions and Comments
	(Comments): Further clarification is needed to ensure that the provision is interpreted in a technologically neutral manner and does not unintentionally exclude secure and widely used identity verification solutions. In particular, it would be useful to clarify how this requirement applies to solutions based on encrypted biometric templates or secure server-side verification mechanisms.
(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 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.'	FR (Drafting suggestions): '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 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 **proves to be impossible or** requires **manifestly** 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.' 5. 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 **manifestly** disproportionate effort **or**

Presidency compromise text	Drafting suggestions and Comments
	is technically impossible, 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.' FR (Comments): Les autorités françaises souhaitent reprendre une expression déjà employee ailleurs dans le RGPD qui fait reference à la fois aux efforts disproportionnés et à l'impossibilité technique. Ceci permettrait d'avoir une coherence de seuil. RO (Comments): The text needs a clarification of the notion of "disproportionate effort" (art. 9(5)), including examples relevant to SMEs.
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~~**and, in the case of** requests under Article 15**, where an abusive intention on the part of** ~~because~~ the data subject ~~abuses the rights conferred by this regulation for purposes other than the protection of their data~~**submitting those requests can be demonstrated**, the controller may either:	PL (Drafting suggestions): The notion of "abusive intention" should be interpreted restrictively to ensure that the exception does not lead to disproportionate limitations of data subjects' rights. PL (Comments):

Presidency compromise text	Drafting suggestions and Comments
	Clarifying that an abusive intention must be demonstrated by the controller constitutes an important safeguard and helps reduce the risk of overly discretionary interpretations by controllers. At the same time, further clarification may be useful to ensure that the concept is applied in a consistent and proportionate manner across Member States and does not discourage data subjects from exercising their rights under the GDPR.
(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or	
(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**, or that the request is submitted with an abusive intention**.'	
5. In Article 13, paragraph 4 is replaced by the following:	
'4. Paragraphs 1, 2 and 3 shall not apply where **and insofar as the data subject has the information and where** the personal data ~~have been~~**are** collected in the context of a ~~clear and~~**direct, limited and clearly** circumscribed relationship between data subjects and a controller exercising an activity that is not ~~data-intensive~~**likely to result in a high risk to the rights and freedoms of data subjects nor involve the processing of large amounts of personal data, special categories of personal data or complex processing operations** and there are reasonable grounds to assume that the	PL (Drafting suggestions): The scope of the exemption should remain strictly limited to genuinely simple and low-risk processing situations in order to ensure that the transparency principle laid down in Article 5(1)(a) GDPR is not undermined. PL

Presidency compromise text	Drafting suggestions and Comments
data subject already has the information referred to in points (a) and (c) of paragraph 1~~, unless~~**.** **The first subparagraph shall not apply where** the controller **intends to process the data collected from the data subject for other purposes,** 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.'	(Comments): The revised wording introduces additional objective elements such as the absence of high risk, the absence of large-scale processing and the exclusion of special categories of personal data or complex processing operations. These elements improve legal certainty and respond to concerns about overly vague concepts in the previous wording. At the same time, the exemption should remain subject to a restrictive interpretation in order to ensure consistency with the transparency principle under Article 5(1)(a) GDPR and the clarifications provided in Recital 36.
6. In Article 13, paragraph 5 is added:	
'5. When the **further** processing takes place for scientific research purposes **by the same controller and where and insofar as**~~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 **further** processing**, subject to the conditions and safeguards referred to in Article 89(1)**, 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.'	FR (Comments): Les autorités françaises soutiennent les modifications apportées à cet article. PL (Drafting suggestions): The concept of "disproportionate effort" should be interpreted restrictively and assessed in light of its impact on the rights and freedoms of data subjects, in line with the safeguards provided for in Article 89 GDPR. PL (Comments): The clarification that the exemption applies only where further processing for scientific research purposes is carried out by the same controller strengthens legal certainty and reduces the risk of an overly broad application of the derogation. At the same time, the application of this exemption should remain exceptional and subject to a case-by-case assessment, taking into account the

Presidency compromise text	Drafting suggestions and Comments
	safeguards laid down in Article 89 GDPR and the interpretative guidance reflected in Recital 37.
~~7.~~ ~~In Article 22, paragraphs 1 and 2 are replaced by the following:~~	FR (Comments): La France soutient le maintien de la rédaction actuelle de l'article 22 et le principe d'une interdiction, assortie d'une dérogation. PL (Drafting suggestions): Poland does not support the deletion of changes to article 22 as it removes the opportunity to clarify the conditions under which decisions based solely on automated processing may be taken and should therefore be reconsidered with a view to providing targeted clarifications while preserving the exceptional nature of such decisions. PL (Comments): Article 22 GDPR constitutes an important safeguard against the potentially harmful effects of fully automated decision-making, including risks of discrimination, algorithmic bias and the absence of meaningful human oversight. While Poland expressed concerns regarding the wording of the original proposal, in particular the formulation suggesting that automated decisions could be taken "regardless of whether the decision could be taken otherwise than by solely automated means", the complete deletion of the proposed amendment removes the possibility of improving legal certainty in this area. In Poland's view, further work could focus on clarifying the interpretation of the "necessity" criterion under Article 22(2)(a), ensuring that fully automated decisions remain exceptional and are subject to appropriate safeguards consistent with the risk-based approach of the GDPR.

Presidency compromise text	Drafting suggestions and Comments
~~'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;~~	
~~(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.'~~	
	FR (Drafting suggestions): **<u>7a. Article 24 is amended as follows:</u>** **<u>(a) paragraph 1 is replaced by the following:</u>** '1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, **with particular regard to the lists referred to in Article 35(4) and (5),** the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.' **<u>7b. Article 25 is amended as follows:</u>**

Presidency compromise text	Drafting suggestions and Comments
	(a) paragraph 1 is replaced by the following: '1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, **with particular regard to the lists referred to in Article 35(4) and (5),** the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.' **7c. Article 32 is amended as follows:** **(a) paragraph 1 is replaced by the following:** '1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, **with particular regard to the lists referred to in Article 35(4) and (5),** the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymisation and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

Presidency compromise text	Drafting suggestions and Comments
	(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.' **(b) the following paragraph is added:** **'5. The Board shall publish guidance for the purpose of further specifying the appropriate technical and organisational measures to ensure a level of security appropriate to the level of risk linked to the different types of processings as mentioned in paragraph 1.'** FR (Comments): Certains aspects du RGPD reflètent déjà le principe de l'approche fondée sur les risques, selon lequel les mesures organisationnelles et techniques que les responsables du traitement et les sous-traitants sont tenus de mettre en place doivent être proportionnées aux risques que présente un traitement de données pour les droits et libertés des personnes concernées. Toutefois, les autorités françaises insistent sur le fait que cette notion, dans son état actuel, n'offre pas aux responsables du traitement suffisamment de clarté et de prévisibilité quant à l'adéquation des mesures qu'ils doivent mettre en place. Les amendements ajoutent des références spécifiques aux listes des opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est ou n'est pas requise aux articles 35, paragraphes 4 et 5, dans tous les articles liant les obligations des responsables du traitement au niveau de risque, et chargent le Comité de publier des lignes directrices précisant les mesures organisationnelles et techniques appropriées pour

Presidency compromise text	Drafting suggestions and Comments
	garantir un niveau de sécurité adéquat en fonction de la classification d'une opération de traitement comme présentant un risque ou un risque élevé pour les personnes physiques. Cela renforcera la prévisibilité, la sécurité juridique et la simplification pour les responsables du traitement et les sous-traitants en rendant transparentes les attentes claires concernant les mesures organisationnelles et techniques à mettre en œuvre, en fonction du niveau de risque associé à une opération de traitement de données donnée. Ainsi, ces modifications apportées aux articles 24, 25, 30 et 32 mettent pleinement en œuvre l'approche fondée sur les risques dans le RGPD.
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~~**72** hours after having become aware of it, 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	PL (Drafting suggestions): Introducing two different deadlines (72 hours and 96 hours) within the same provision creates legal uncertainty, while extending the notification deadline to 96 hours would provide a clearer and more practical framework for controllers. PL

Presidency compromise text	Drafting suggestions and Comments
of this Regulation. Where the notification to the supervisory authority is not made within 96 hours, it shall be accompanied by reasons for the delay.'	(Comments): Poland strongly supports extending the deadline for notifying personal data breaches from 72 to 96 hours, as this change would better reflect the practical realities of incident response and is widely expected by stakeholders. The current compromise text introduces both a 72-hour notification deadline and a 96-hour reference period within the same provision. This solution may create legal uncertainty for controllers when determining the applicable timeframe and therefore does not provide the intended simplification. A single and clearly defined 96-hour deadline would provide greater legal certainty while maintaining an effective level of protection for data subjects and ensuring timely notification to supervisory authorities. RO (Comments): . The text needs clarification regarding the establishment of the notification deadline in the event of a data breach (96 hours or 72 hours?)
(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 **of this Regulation**.'	PL (Drafting suggestions): The coordination between the establishment of the single-entry point under Directive (EU) 2022/2555 and the notification obligations under Article 33 GDPR should be clearly defined to avoid procedural uncertainty during the transitional period.
(c) the following paragraphs are added:	

Presidency compromise text	Drafting suggestions and Comments
'6. The Board shall ~~prepare and transmit to the Commission a proposal for~~**establish and make public** 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 **and a list of the circumstances in which it is not likely to result in such a high risk. The template and lists**~~. The proposals~~ shall be ~~submitted to the Commission~~**available** 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).~~	PL (Drafting suggestions): Poland supports to have the template adopted by the way of the implementing act. Only through this is can be ensured that the template is used in all 27 MS. Therefore Poland does not support the proposed changes. Poland also supports the empowerment for the implementing act to adopt the list of circumstances in which a personal data breach is likely to result in a high risk to the rights and freedom of a natural person. Further clarification may be needed to ensure that the lists of circumstances related to "high risk" serve as interpretative guidance and do not replace the controller's obligation to carry out an individual risk assessment.
7. The template and ~~the list~~**lists** 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.'~~	PL (Drafting suggestions): Comment as above, PL does not support the changes
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~~**establish and make public** a list of the kind of processing operations	PL (Drafting suggestions):

Presidency compromise text	Drafting suggestions and Comments
which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1.	Poland does not support the changes. We welcomed the empowerment for implementing act to ensure aligned implementation in all MS. PL asks to revert to the COM proposal. The establishment of EU-level lists and a common DPIA template and methodology should not affect the controller's obligation to carry out an individual risk assessment in accordance with the risk-based approach underpinning the GDPR. PL (Comments): At the same time, it remains important that the application of such lists and methodologies does not replace the need for an individual assessment of risks by controllers, in line with the risk-based approach underpinning the GDPR and the clarification provided in Recital 40.
5. The Board shall ~~prepare and transmit to the Commission a proposal for~~**establish and make public** a list of the kind of processing operations for which no data protection impact assessment is required.	PL (Drafting suggestions): Comment as above
6. The Board shall ~~prepare and transmit to the Commission a proposal for~~**establish and make public** a common template and a common methodology for conducting data protection impact assessments.'	PL (Drafting suggestions): Comment as above RO (Drafting suggestions): light DPIA templates RO

Presidency compromise text	Drafting suggestions and Comments
	(Comments): In order to support the coherent and proportionate application of data protection impact assessment obligations, in particular for small and medium-sized enterprises, it is appropriate to develop simplified assessment models ("light DPIA templates")
(b) the following ~~paragraphs are~~**paragraph is** inserted:	FR (Drafting suggestions): (b) the following **paragraphs are** inserted: PL (Drafting suggestions): Comment as above
~~'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).~~	FR (Drafting suggestions): **'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 published within [OP date = 9 months of the entry into application of this Regulation].'** FR (Comments): Les autorités françaises estiment que le maintien d'un délai est nécessaire ici. PL (Drafting suggestions): Comment as above

Presidency compromise text	Drafting suggestions and Comments
~~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 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.~~	FR (Drafting suggestions): 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 adopt any updates. FR (Comments): Là aussi, les autorités françaises estiment qu'il est utile de prévoir la mise à jour régulière. PL (Drafting suggestions): Comment as above
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~~**Board establishes and makes public the lists** referred to in paragraph ~~6a~~**4 and 5**.'	PL (Drafting suggestions): Comment as above
10. ~~The following article is added:~~	
~~'Article 41a~~	

Presidency compromise text	Drafting suggestions and Comments
~~(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.~~	PL (Drafting suggestions): Poland does not support the deletion of Article 41a as it removes the possibility to clarify the role of pseudonymisation and the assessment of re-identification risks under the GDPR and should therefore be reconsidered, while ensuring that such clarification does not relativise the definition of personal data laid down in Article 4(1) of the Regulation. PL (Comments): Poland notes that the complete deletion of Article 41a removes an opportunity to provide additional legal clarity regarding the assessment of re-identification risks in the context of pseudonymised data. Clarification in this area could support controllers in applying privacy-preserving techniques and encourage the use of pseudonymisation as an important safeguard under Article 89 GDPR. At the same time, any future provision in this area should avoid creating a mechanism that would relativise the concept of personal data depending on the category of recipient or automatically qualify pseudonymised data as non-personal. Such an approach could undermine the uniform application of the definition of personal data under Article 4(1) GDPR and create risks of circumvention of data protection rules. In Poland's view, further work could focus on developing criteria and guidance for assessing the risk of re-identification, taking into account the state of the art of available technologies, including artificial intelligence and data-linking capabilities, while preserving the accountability of controllers and the case-by-case assessment required under the GDPR.
~~(2) For the purpose of paragraph 1 the Commission shall:~~	

Presidency compromise text	Drafting suggestions and Comments
~~(a) assess the state of the art of available techniques;~~	
~~(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;	
	FR (Drafting suggestions): **(b) the following paragraph is added:**

Presidency compromise text	Drafting suggestions and Comments
	‘National supervisory authorities shall refrain from adopting guidelines, recommendations and best practices on matters already covered by guidelines, recommendations and best practices issued by the Board and, where necessary, shall update or repeal their national documentation adopted prior to guidelines, recommendations and best practices adopted by the Board in order to ensure consistency of interpretation of this Regulation.’ FR (Comments): Les autorités françaises estiment qu’il est important de rappeler ce point pour assurer la coherence d’interprétation et d’application du RGPD et renforcer la gouvernance assure par le CEPD en la matière.
12. In Article 64(1), point (a) is deleted.	
	FR (Drafting suggestions): **12a. Article 64 is amended as follows:** **(a) the following paragraph is added:** **‘2a. Controllers subject to this Regulation may present a reasoned request that any matter of consistent application directly relevant for them in more than one Member State be examined by the Board with a view to obtaining an opinion on this matter.’** **(b) paragraph 3 and 4 are replaced by the following:** **‘3. In the cases referred to in paragraphs 1, 2 and 2a, the Board shall issue an opinion on the matter submitted to it provided that it has not already issued an opinion on the same matter. That opinion shall be**

Presidency compromise text	Drafting suggestions and Comments
	adopted within eight weeks by simple majority of the members of the Board. That period may be extended by a further six weeks, taking into account the complexity of the subject matter. Regarding the draft decision referred to in paragraph 1 circulated to the members of the Board in accordance with paragraph 5, a member which has not objected within a reasonable period indicated by the Chair, shall be deemed to be in agreement with the draft decision. **12b. In Article 65(1), point (c) is replaced by the following:** **'(c) where a competent supervisory authority does not request the opinion of the Board in the cases referred to in Article 64(1), or does not follow the opinion of the Board issued under Article 64. In that case, any supervisory authority concerned, the Commission or any controller concerned where that opinion was issued on the grounds of a request under Article 64(2a) or of Article 41a may communicate the matter to the Board.'** FR (Comments): Ces modifications visent à étendre aux parties prenantes le mécanisme prévu aux articles 64 et 65, qui permet aux autorités de contrôle nationales de saisir le comité. Elles offrent aux parties prenantes la possibilité de saisir le comité en lui adressant une demande motivée afin d'obtenir un avis ou, en dernier ressort, l'adoption d'une décision contraignante. Les autorités françaises estiment que l'extension de cette possibilité aux parties prenantes soumises au RGPD conduira à une mise en œuvre plus cohérente du RGPD par les autorités nationales de contrôle et garantira l'homogénéité au sein du marché unique. Cela renforcera la sécurité juridique et la prévisibilité pour les acteurs économiques, tout en offrant un mécanisme de recours direct permettant au comité de réagir rapidement et efficacement

Presidency compromise text	Drafting suggestions and Comments
	pour traiter les problèmes liés à l'application cohérente du RGPD dès qu'ils sont identifiés par les parties prenantes. Les autorités françaises souhaitent que l'accès au Comité soit également ouvert aux responsables de traitements et aux sous-traitants pour leur permettre de le saisir de demandes d'avis sur des sujets les concernant directement. Ces amendements permettraient de renforcer la gouvernance par le CEPD et la cohérence d'application du RGPD dans l'Union, en même temps qu'il permettrait d'ouvrir des dialogues entre le CEPD et les responsables de traitements et sous-traitants à leur initiative sur les sujets le méritant.
13. In Article 70(1), point (h) is deleted.	
	FR (Drafting suggestions): **13a. In Article 70(1), point (t) is replaced with the following:** **'(c) issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to in Article 64(1), on matters submitted pursuant to Article 64(2) and (2a), and to issue binding decisions pursuant to Article 65, including in cases referred to in Article 66;'** FR (Comments): Cet amendement actualise le point correspondant des missions du Conseil afin de tenir compte des modifications proposées aux articles 64 et 65.
14. In Article 70(1), the following points are inserted:	
'(ha) ~~prepare and transmit to the Commission a proposal for~~**establish** a list of the kind of processing operations which are subject to the requirement for	

Presidency compromise text	Drafting suggestions and Comments
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~~**establish** 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~~**establish** 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 **and a list of the circumstances in which it is not likely to result in such a high risk**	
hca issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph on pseudonymisation, clarifying circumstances whether a natural person is identifiable and means reasonably likely to be used to identify a natural person, and specifying means and criteria to determine whether data resulting from pseudonymisation may no longer constitute personal data for certain entities'	FR (Drafting suggestions): **hca) adopt an opinion pursuant to Article 64(3) by [OP date = 2 months of the entry into application of this Regulation] to specify means and criteria to determine whether data resulting from pseudonymisation no longer allows the identification of the data subject by for certain entities. For that purpose, it shall assess the state of the art of available techniques and develop criteria and or categories for controllers and recipients to assess the risk of re-identification in relation to typical recipients of data.** FR (Comments):

Presidency compromise text	Drafting suggestions and Comments
	Les autorités françaises estiment qu'il est nécessaire de prévoir ici quelque chose de plus contraignant que des lignes directrices et qu'il faut maintenir un délai pour l'adoption de ces éléments sur la pseudonymisation. Il est indispensable que le CEPD fournisse au plus vite des éléments concrets aux responsables de traitements pour appliquer la jurisprudence de la CJUE. Ces éléments doivent en outre pouvoir être rendus opposables aux autorités de contrôle. C'est pourquoi les autorités françaises proposent l'adoption d'un avis plutôt que de lignes directrices sur un sujet aussi central que la notion de données identifiantes. PL (Drafting suggestions): Amend point (hca) to clarify that guidance on pseudonymisation should support the assessment of identifiability without affecting the definition of personal data laid down in Article 4(1) GDPR and without automatically qualifying pseudonymised data as non-personal data. Proposed wording: (hca) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph on pseudonymisation, including guidance on assessing whether a natural person is identifiable and on the means reasonably likely to be used to identify a natural person, as well as on the criteria and technical and organisational measures relevant for assessing re-identification risks in relation to pseudonymised data, without affecting the definition of personal data laid down in Article 4(1) of this Regulation. PL (Comments): Poland notes that entrusting the European Data Protection Board with the task of developing guidance and practical tools may contribute to a more consistent application of the GDPR across the Union, in particular with regard to data protection impact assessments and personal data breach notifications.

Presidency compromise text	Drafting suggestions and Comments
	At the same time, point (hca) touches upon the concept of identifiability and the legal effects of pseudonymisation, which are closely linked to the definition of personal data laid down in Article 4(1) GDPR. In Poland's view, it is important to ensure that any guidance issued by the Board in this area remains consistent with Recital 26 GDPR and does not lead to a reinterpretation of the concept of personal data. In particular, guidance on pseudonymisation should assist controllers and recipients of data in assessing re-identification risks and identifiability in specific contexts, without introducing the concept of "relative personal data" or leading to an automatic qualification of pseudonymised data as non-personal data. Clarifying this point would ensure coherence with the systemic structure of the GDPR and with the safeguards proposed in relation to pseudonymisation in other provisions of the Regulation.
	FR (Drafting suggestions): **'(he) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for the purpose of further specifying the appropriate technical and organisational measures to ensure a level of security appropriate to the level of risk pursuant to Article 32(5);'** FR (Comments): Cet amendement actualise la liste des missions du Conseil à la suite de la proposition d'amendement visant à introduire un paragraphe 5 à l'article 32, qui charge le Conseil d'adopter des lignes directrices précisant davantage les mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité adapté au niveau de risque.
15. After Article 88, the following articles are added:	FR (Drafting suggestions):

Presidency compromise text	Drafting suggestions and Comments
	~~15. After Article 88, the following articles are added:~~
‘Article 88a	FR (Drafting suggestions): ~~‘Article 88a~~ FR (Comments): Même commentaire que supra, les dispositions de la Directive ePrivacy n’ont pas vocation à intégrer le RGPD qui concerne les règles applicables aux traitements de données, et pas celles applicables aux opérations techniques pouvant conduire au traitement subséquent de données à caractère personnel. Le consentement au dépôt des cookies ne peut pas s’assimiler au consentement au traitement des données, ni offrir les mêmes droits à l’issue du dépôt que le consentement au traitement de données. Ainsi, par exemple, le dépôt de cookies ne doit pas conduire à l’ouverture d’un droit à la portabilité des cookies, d’un droit d’accès ou d’un droit à l’oubli à l’égard des cookies eux-mêmes, qui n’auraient aucun sens. Appliquer tout le régime du RGPD aux traceurs n’aurait aucun sens et créerait des difficultés d’autant plus fortes que le projet d’omnibus maintient l’article 5, paragraphe 3 de la Directive ePrivacy par ailleurs lorsque les traceurs n’entraînent pas de traitements de données personnelles. C’est pourquoi les autorités françaises estiment que les amendements devraient être apportés à l’article 5, paragraphe 3 de la Directive ePrivacy pour l’ensemble des traceurs, sans instituer deux régimes.
Processing of personal data in the terminal equipment of natural persons	FR (Drafting suggestions): ~~Processing of personal data in the terminal equipment of natural persons~~

Presidency compromise text	Drafting suggestions and Comments
(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.	FR (Drafting suggestions): ~~(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.~~
(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).	FR (Drafting suggestions): ~~(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).~~
(3) 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:	FR (Drafting suggestions): ~~(3) 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 prévoir dans la directive ePrivacy elle-même. FR (Comments):

Presidency compromise text	Drafting suggestions and Comments
	Les autorités françaises sont néanmoins favorables à étudier ces propositions d'assouplissements mais dans le contexte de la Directive ePrivacy ou d'un autre instrument.
(a) carrying out the transmission of an electronic communication over an electronic communications network;	FR (Drafting suggestions): ~~(a) carrying out the transmission of an electronic communication over an electronic communications network;~~ A prévoir dans la directive ePrivacy elle-même.
(b) providing a service explicitly requested by the data subject;	FR (Drafting suggestions): ~~(b) providing a service explicitly requested by the data subject;~~ A prévoir dans la directive ePrivacy elle-même.
(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;	FR (Drafting suggestions): ~~(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;~~ A prévoir dans la directive ePrivacy elle-même. FR

Presidency compromise text	Drafting suggestions and Comments
	(Comments): Sous la réserve liminaire que ces modifications ne soient pas intégrées au RGPD mais à la directive ePrivacy, les autorités françaises sont favorables à introduire une exemption supplémentaire pour la mesure d'audience. Celle-ci devrait par ailleurs être étendue pour inclure les organismes de mesure agissant en tant que responsables conjoints de traitement ou sous-traitants du service sollicité par la personne concernée.
(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.	FR (Drafting suggestions): ~~(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.~~ A prévoir dans la directive ePrivacy elle-même. FR (Comments): Là encore, sous la réserve liminaire que ces modifications ne soient pas intégrées au RGPD mais à la directive ePrivacy, les autorités françaises sont favorables à introduire une exemption supplémentaire en matière de sécurité dans la mesure où cet objectif paraît opportun et légitime. Une telle exemption devrait être limitée à ce qui est nécessaire à la sécurité du système informatique et du traitement de données concernés, et sous les réserves que l'utilisateur est informé de cette opération technique et qu'il peut désactiver les installations automatiques de ces composants.

Presidency compromise text	Drafting suggestions and Comments
(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:	FR (Drafting suggestions): ~~(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:~~ A prévoir dans la directive ePrivacy elle-même.
(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;	FR (Drafting suggestions): ~~(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;~~ A prévoir dans la directive ePrivacy elle-même.
(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;	FR (Drafting suggestions): ~~(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;~~ A prévoir dans la directive ePrivacy elle-même.
(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.	FR (Drafting suggestions): ~~(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.~~

Presidency compromise text	Drafting suggestions and Comments
	A prévoir dans la directive ePrivacy elle-même.
This paragraph also applies to the subsequent processing of personal data based on consent.	FR (Drafting suggestions): ~~This paragraph also applies to the subsequent processing of personal data based on consent.~~
(5) This Article shall apply from [OP: please insert the date = 6 months following the date of entry into force of this Regulation]	FR (Drafting suggestions): ~~(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	FR (Drafting suggestions): ~~Article 88b~~ FR (Comments): Si les autorités françaises perçoivent l'objectif de cette proposition, celle-ci soulève en pratique des difficultés techniques innombrables qui conduisent à demander la suppression de cette disposition. En effet, d'une part, de la même manière que concernant l'article 88a, il s'agit ici de règles techniques relatives aux traceurs, qui n'ont pas à figurer dans le RGPD. D'autre part, malgré l'exemption proposée pour la presse, ces propositions suscitent de très importantes difficultés aussi pour ce secteur qui se trouverait

Presidency compromise text	Drafting suggestions and Comments
	mis en difficulté du fait de sa singularisation et de son exclusion de la sphère en circuit fermé opérée par des opérateurs qui fournissent à la fois les plateformes de navigation et participent à la chaîne de valeur la publicité en ligne. Cette proposition, dont les autorités françaises peinent à analyser complètement les impacts et potentiels effets de bord du fait de l'absence d'analyse d'impact de la proposition de règlement omnibus, conduit en tout état de cause à des modifications très structurantes du cadre réglementaire qu'il convient de mieux évaluer avant de procéder à l'ajout d'un article dans un cadre législatif portant sur un domaine différent et qui n'est pas le plus adapté. Les autorités françaises demandent donc la suppression de cet article. PL (Comments): Comments will be shared later
Automated and machine-readable indications of data subject's choices with respect to processing of personal data in the terminal equipment of natural persons	FR (Drafting suggestions): ~~Automated and machine-readable indications of data subject's choices with respect to processing of personal data in the terminal equipment of natural persons~~
(1) Controllers shall ensure that their online interfaces allow data subjects to:	FR (Drafting suggestions): ~~(1) Controllers shall ensure that their online interfaces allow data subjects to:~~ RO

Presidency compromise text	Drafting suggestions and Comments
	(Comments): :
(a) Give consent through automated and machine-readable means, provided that the conditions for consent laid down in this Regulation are fulfilled;	FR (Drafting suggestions): ~~(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.	FR (Drafting suggestions): ~~(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.	FR (Drafting suggestions): ~~(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.	FR (Drafting suggestions): ~~(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	FR (Drafting suggestions):

Presidency compromise text	Drafting suggestions and Comments
organisations to draft standards for the interpretation of machine-readable indications of data subjects' choices.	~~(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 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.	FR (Drafting suggestions): ~~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].	FR (Drafting suggestions): ~~(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.	FR (Drafting suggestions): ~~(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.~~

Presidency compromise text	Drafting suggestions and Comments
(7) Paragraph 6 shall apply from [OP: please insert the date = 48 months following the date of entry into force of this Regulation].	FR (Drafting suggestions): ~~(7) Paragraph 6 shall apply from [OP: please insert the date = 48 months following the date of entry into force of this Regulation].~~
Article 88c	
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.	RO (Comments): .
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 data subjects with an unconditional right to object to the processing of their personal data.’	

Presidency compromise text	Drafting suggestions and Comments
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:	
(a) Article 2, point (1);	
(b) Article 2, point (2);	
(c) Article 2, point (5);	
(d) Article 4;	
(e) Article 11;	
(f) Article 15.	