The Digital Omnibus
Suggested amendments

Article 4(38) – scientific research

Text proposed by the Commission	*Amendments*
Article 4 (38) "scientific research" means any research which can also support innovation, such as technological development and demonstration. These actions shall contribute to existing scientific knowledge or apply existing knowledge in novel ways, be carried out with the aim of contributing to the growth of society´s general knowledge and wellbeing and adhere to ethical standards in the relevant research area. This does not exclude that the research may also aim to further a commercial interest.'	Article 4 (38) "scientific research" means any research which can ~~also support innovation, such as technological development and demonstration. These actions shall~~ contribute to existing scientific knowledge or apply existing knowledge in novel ways.~~,~~ **It should** 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.'

Justification

The text could be read to only support research carried out for the sole aim of contributing to the growth of society´s general knowledge and wellbeing which could lead to an overly narrow interpretation.

Article 9.2(k) & 9.5 – incidental and residual processing of special categories of personal data in the context of the development and operation of an AI system

Text proposed by the Commission	*Amendments*
Article 9.5 (new) 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	Article 9.5 (new) 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~~ **across the AI development lifecycle to ensure the effective protection** of **the** 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~~ **when their**

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.'	**deletion or anonymization would be impossible or entail a** 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.'~~
Recital 33: ….The derogation should only apply where the controller has implemented appropriate technical and organisational measures in an effective manner to avoid the processing of those data, takes the appropriate measures during the entire lifecycle of an AI system or AI model and, once it identifies such data, effectively remove them. If removal would require disproportionate effort, notably where the removal of special categories of data memorised in the AI system or AI model would require re-engineering the AI system or AI model, the controller should effectively protect such data 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.	Recital 33: …The derogation should only apply where the controller has implemented appropriate technical and organisational measures **across the AI development lifecycle** ~~in an effective manner~~ **to ensure the effective protection of the special categories of data when their deletion or anonymization would be impossible or entail a disproportionate effort** ~~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) and Article 10 of Regulation (EU) 2016/679.

Justification

The requirement to avoid the collection and processing of special categories of personal data and, where identified, to remove or isolate it, is disproportionate. Controllers would be obliged to continuously monitor the input of a dataset for special categories of data which due to its complexity and size would render the development or operation of an AI system under this legal basis impossible.

Processing in the context of the development and operation of an AI system

Text proposed by the Commission	*Amendments*
Article 88c: 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	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),

Article 3, point (1), of Regulation (EU) 2024/1689 or an AI model, such processing may be pursued for legitimate interests within the meaning of Article 6(1)(f) of Regulation (EU) 2016/679, where appropriate, except where other Union or national laws explicitly require consent, and where such interests are overridden by the interests, or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. Any such processing shall be subject to appropriate organisational, technical measures and safeguards for the rights and freedoms of the data subject, such as to ensure respect of data minimisation during the stage of selection of sources and the training and testing of AI an system or AI model, to protect against non-disclosure of residually retained data in the AI system or AI model to ensure enhanced transparency to data subjects and providing data subjects with an unconditional right to object to the processing of their personal data.'	of Regulation (EU) 2024/1689 or an AI model, such processing may be pursued for legitimate interests within the meaning of Article 6(1)(f) of Regulation (EU) 2016/679, where appropriate, except ~~where other Union or national laws explicitly require consent, and~~ where such interests are overridden by the interests, or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. Any such processing shall be subject to appropriate organisational, technical measures and safeguards for the rights and freedoms of the data subject, such as to ensure respect of data minimisation during the stage of selection of sources and the training and testing of AI an system or AI model, to protect against non-disclosure of residually retained data in the AI system or AI model to ensure ~~enhanced~~ transparency to data subjects and providing data subjects with **the** ~~an unconditional~~ right to object to the processing of their personal data **as defined in Article 21.1 of Regulation (EU) 2016/679**.
Recital 31: …. 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.	Recital 31: …. 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~~ **ensuring the data subject's** 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.

Justification

Processing for the development and operation of an AI system usually requires large data sets and a reliable legal basis. It would be impossible to reconcile such processing with different national

procedures requiring consent for specific datasets. Furthermore, the legitimate interests basis already mandates robust accountability, so that it would suffice to align the transparency requirements in this context with the information that has to be legally provided according to Articles 13 and 14 GDPR and the right to object in Article 88c with the rules as set out by Article 21(1) GDPR.

Limitation to data subject access requests

Text proposed by the Commission	*Amendments*
Article 12.5 5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character or also, for requests under Article 15 because the data subject abuses the rights conferred by this regulation for purposes other than the protection of their data, the controller may either: (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or (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.	Article 12.5 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 **where an abusive intention on the part of the data subject submitting those requests can be demonstrated** ~~also, for requests under Article 15 because the data subject abuses the rights conferred by this regulation for purposes other than the protection of their data~~, the controller may either: (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or (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.
Recital 35 …By contrast, it should be clarified in Article 12 of the Regulation that the right of access, which is from the outset favourable to data subjects, should not be abused in the sense that the data subjects abuse them for purposes other than the protection of their data. For example, such an abuse of the right of access would arise where the data subject intends to cause the controller to refuse an access request, in order to subsequently demand the payment of compensation, potentially under the threat of bringing a claim for damages. Other examples of abuse include situations where data subjects make excessive	Recital 35 …By contrast, it should be clarified in Article 12 of the Regulation that exercise of the right of access **can be considered excessive where an abusive intention on the part of the data subject submitting those requests can be demonstrated by the controller.**, ~~which is from the outset favourable to data subjects, should not be abused in the sense that the data subjects abuse them for purposes other than the protection of their data.~~ For example, such an abus**esive intention** ~~of the right of access~~ would arise where the data subject intends to cause the controller to refuse an access request, in order to subsequently demand the payment

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

Justification

The EDPB and the EDPS have argued that the notion of abuse of rights should not be linked with the exercise of the right to access for purposes other than data protection and propose to link it with the existence of an abusive intention, e.g., evident intention to cause harm to the controller. It is important to retain the lower threshold of 'reasonable grounds to believe' in relation to the burden of proof, as controllers rarely if ever have conclusive evidence of a data subject's true intent and have to make reasonable inferences based on circumstances.

Articles 33 – Data breach notification

Text proposed by the Commission	*Amendments*
Article 33.1 In the case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall without undue delay and, where feasible, not later than 96 hours after having	Article 33.1 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 **4 working days** ~~96 hours~~

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. Where the notification to the supervisory authority is not made within 96 hours, it shall be accompanied by reasons for the delay.	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. Where the notification to the supervisory authority is not made within **4 working days** ~~96 hours~~, it shall be accompanied by reasons for the delay.
Article 33.6 The Board shall prepare and transmit to the Commission a proposal for a common template for notifying a personal data breach to the competent supervisory authority referred to in paragraph 1 as well as for a list of the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person. The proposals shall be submitted to the Commission within [OP date = nine months of the entry into application of this Regulation]. The Commission after due consideration reviews it, as necessary, and is empowered to adopt it by way of an implementing act in accordance with the examination procedure set out in Article 93(2).	Article 33.6 The Board shall **establish and make public** ~~prepare and transmit to the Commission a proposal for~~ a common template for notifying a personal data breach to the competent supervisory authority referred to in paragraph 1 as well as ~~for~~ a list of the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person. The **template and list** ~~proposals~~ shall be available ~~submitted to the Commission~~ within [OP date = nine months of the entry into application of this Regulation]. ~~The Commission after due consideration reviews it, as necessary, and is empowered to adopt it by way of an implementing act in accordance with the examination procedure set out in Article 93(2).~~
Article 33.7 The template and the list referred to in paragraph 6 shall be reviewed at least every three years and updated where necessary. The Board shall submit its assessment and possible proposals for updates to the Commission in due time. The Commission after due consideration of the proposals reviews them and is empowered to adopt any updates following the procedure in paragraph 6.	Article 33.7 The template and the list referred to in paragraph 6 shall be reviewed at least every three years and updated where necessary. ~~The Board shall submit its assessment and possible proposals for updates to the Commission in due time. The Commission after due consideration of the proposals reviews them and is empowered to adopt any updates following the procedure in paragraph 6.~~
Recital 39 … In order to facilitate compliance by controllers and a harmonised approach in the Union, the Board should prepare a common template for notifying data breaches to the competent supervisory authority and a common list of circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person. The Commission should take due account of the proposal prepared by the Board and review them, as necessary, prior to	Recital 39 … In order to facilitate compliance by controllers and a harmonised approach in the Union, the Board should **establish and make public** ~~prepare~~ a common template for notifying data breaches to the competent supervisory authority and a common list of circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person. ~~The Commission should take due account of the proposal prepared by the Board and review them, as~~

adoption. In order to take account of new information security threats, the common template and the list should be reviewed at least every three years and updated where necessary. The lack of a common list of circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person should not affect the obligations of controllers to notify those breaches.	~~necessary, prior to adoption.~~ In order to take account of new information security threats, the common template and the list should be reviewed at least every three years and updated where necessary. The lack of a common list of circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person should not affect the obligations of controllers to notify those breaches.

Justification

The common notification template and list of the high-risk circumstances should not be adopted as a mandatory measure as it needs to guarantee sufficient flexibility allowing gradual implementation over time and in different technological environments.

Articles 35 – Data protection impact assessments

Text proposed by the Commission	*Amendments*
Article 35.6: The Board shall prepare and transmit to the Commission a proposal for a common template and a common methodology for conducting data protection impact assessments.	Article 35.6: The Board shall **establish and make public** ~~prepare and transmit to the Commission a proposal for~~ a common template and a common methodology for conducting data protection impact assessments.
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).	6a. The ~~proposals for~~ lists referred to in paragraphs 4 and 5 and for the template and methodology referred to in paragraph 6 shall be **available** ~~submitted to the Commission~~ within [OP date = 9 months of the entry into application of this Regulation]. ~~The Commission after due consideration reviews them, as necessary, and is empowered to adopt them by way of an implementing act in accordance with the examination procedure set out in Article 93(2).~~
6b. The lists and the template and methodology referred to in paragraph 6a- shall be reviewed at least every three years and updated where necessary. The Board shall submit its assessment 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.	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.~~

Recital 40 … The lists of processing operations should be prepared by the Board and adopted by the Commission as an implementing act. In In order to facilitate compliance by controllers, the Board should also prepare a common template and a common methodology for conducting data protection impact assessments, to be adopted by the Commission as an implementing act. The Commission should take due account of the proposals prepared by the Board and review them, as necessary, prior to adoption. In order to take account of technological developments, the lists and the common template and methodology should be reviewed at least every three years and updated where necessary.	Recital 40 … The lists of processing operations should be **established and made public** ~~prepared~~ by the Board ~~and adopted by the Commission as an implementing act.~~ In order to facilitate compliance by controllers, the Board should also **establish and make public** ~~prepare~~ a common template and a common methodology for conducting data protection impact assessments~~, to be adopted by the Commission as an implementing act. The Commission should take due account of the proposals prepared by the Board and review them, as necessary, prior to adoption.~~ In order to take account of technological developments, the lists and the common template and methodology should be reviewed at least every three years and updated where necessary.

Justification

The common notification template and methodology should not be adopted as a mandatory measure as it needs to guarantee sufficient flexibility allowing gradual implementation over time and in different technological environments.

Article 88a: Integration of the cookie rules into the GDPR

Text proposed by the Commission	*Amendments*
Article 88a: Storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person without consent, and subsequent processing, shall be lawful to the extent it is necessary for any of the following: (a) carrying out the transmission of an electronic communication over an electronic communications network; (b) providing a service explicitly requested by the data subject; (c) creating aggregated information about the usage of an online service to measure the audience of such a service, where it is carried out by the controller of that online service solely for its own use; (d) maintaining or restoring the security of a service provided by the controller and requested by the data subject or the terminal	**Article 5.3 of Directive 2002/58/EC: Member States shall ensure that the** ~~S~~storing of ~~personal data~~ **information**, or gaining of access to ~~personal data~~ **information** already stored, in the terminal equipment of a ~~natural person~~ **subscriber or user** without consent, and subsequent processing, shall be lawful to the extent it is necessary for any of the following: (a) carrying out the transmission of an electronic communication over an electronic communications network; (b) providing a service explicitly requested by the data subject; (c) creating aggregated information about the usage of an online service to measure the audience of such a service, where it is carried out by the controller of that online service ~~solely for its own use~~;

equipment used for the provision of such service.	(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, **including the detection and prevention of unauthorised or malicious conduct.** **(e) allowing the delivery, billing and measurement of advertising made solely on the basis of the immediate content displayed on the user's interface and not based on any type of profiling.**

Justification

The rules on storing of information, or the gaining of access to information already stored, in the terminal equipment of a user should not be transferred to the GDPR as this creates a duplicated consent regime whereby the user may need to consent twice as cookies do not distinguish between personal and non-personal data. The exceptions to the consent rule should be further clarified and expanded. Maintaining the security of a service goes beyond the technical system security and should include the detection and prevention of other activities antagonistic to the use of the service, such as unauthorised or malicious conduct. Requiring in this case separate consent whereby users may decline and create vulnerabilities would not make sense. Finally, an additional exception should allow low-risk contextual advertising models to operate without consent provided that they are not based on any type of profiling.

Article 88b: automated and machine-readable indications of data subjects' choices

Text proposed by the Commission	*Amendments*
Article 88b: Controllers shall ensure that their online interfaces allow data subjects to: (a) Give consent through automated and machine-readable means, provided that the conditions for consent laid down in this Regulation are fulfilled; (b) decline a request for consent and exercise the right to object pursuant to Article 21(2) through automated and machine-readable means. (2) Controllers shall respect the choices made by data subjects in accordance with paragraph 1 (3) Paragraphs 1 and 2 shall not apply to controllers that are media service providers when providing a media service. (4) The Commission shall, in accordance with Article 10(1) of Regulation (EU) 1025/2012,	**deleted**

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. (5) Paragraphs 1 and 2 shall apply from [OP: please insert the date = 24 months following the date of entry into force of this Regulation]. (6) Providers of web browsers, which are not SMEs, shall provide the technical means to allow data subjects to give their consent and to refuse a request for consent and exercise the right to object pursuant to Article 21(2) through the automated and machine-readable means referred to in paragraph 1 of this Article, as applied pursuant to paragraphs 2 to 5 of this Article. (7) Paragraph 6 shall apply from [OP: please insert the date = 48 months following the date of entry into force of this Regulation].	

Justification

A centralised and automated consent mechanism that provides blanket privacy settings would not comply with the GDPR's definition of consent. It would also remove any incentive for third party providers to innovate and offer better privacy-friendly services than their competitors which may result in less rather than more protection of users' privacy. It would deprive consumers of the ability to share more data with the specific companies that they trust.

About Video Games Europe

Since 1998, Video Games Europe has ensured that the voice of a responsible video games ecosystem is heard and understood. Its mission is to support and celebrate the sector's creative and economic potential and to ensure that players around the world enjoy the benefits of great video game playing experiences. Europe's video games sector is worth €26.8bn and accounts for 116,419 jobs. 54% of Europeans are video game players. We publish a yearly Key Facts report with the latest data on Europe's video games sector.

www.videogameseurope.eu