WILLIAM FRY

// Technology

EU Digital Omnibus – Key GDPR Proposals

December 2025

The European Commission released its Digital Omnibus Package on 19 November 2025, a reform that seeks to overhaul significant parts of the EU's digital regulatory framework. In our table below, we highlight some of the key changes proposed by the Digital Omnibus as they relate to the General Data Protection Regulation (GDPR) and their effects, if implemented.

GDPR Articles affected by the Proposal	Digital Omnibus Proposal Reference	GDPR's Current Text	Omnibus Proposal Amendment (Emphasis added)	What is being changed?	What does this mean?
Article 4(1) (Definition of Personal Data)	Article 3(1)(a) and 3(10)	'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;"	*The following is added to the end of the existing definition:* **'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.'** *Additionally, under a new Article 41a, the Commission would be empowered to adopt implementing acts to specify means and criteria to determine whether data resulting from pseudonymisation no longer constitutes personal data for certain entities (such that controllers*	The definition of personal data is clarified, codifying Court of Justice of the European Union case law on identifiability and pseudonymisation, so that if a given entity does not have the means to identify someone from the data they hold (considering the means reasonably likely to be used by them), it is not considered personal data. This is irrespective of whether a subsequent holder of the data may be later able to identify individuals. See also *European Data Protection Supervisor v Single*	Provides clarity as to the scope of personal data within the meaning of the GDPR. Identifiability of an individual from data must be assessed contextually, on a case-by-case basis, from the perspective of a given entity processing the data (e.g. a data holder), and that pseudonymised data may, under certain conditions, fall outside the scope of the definition of personal data under the GDPR (and therefore, potentially meaning that GDPR obligations, such as the requirement for Article 28

GDPR Articles affected by the Proposal	Digital Omnibus on AI Proposal Reference	GDPR's Current Text	Omnibus Proposal Amendment (Emphasis added)	What is being changed?	What does this mean?
			will understand the means and criteria to demonstrate that data cannot lead to re-identification of data subjects).	*Resolution Board* Case C-2025/645 (here and here).	data protection clauses, may not apply to such data).
New Article 88c (Processing in the context of the development and operation of AI)	Article 3(15)	*No equivalent provision. This would be a* **new** *legislative provision in the GDPR.*	*A new Article 88c is inserted:* **"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 the AI Act] … 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."**	Expressly recognises legitimate interests as a legal basis for the development and operation of AI systems and models, where appropriate and subject to appropriate organisational, technical measures and safeguards for the rights and freedoms of the data subject.	Expressly allows controllers to rely on the legal basis of 'necessity for legitimate interests' to train and/or operate AI systems and models which may process personal data (without needing consent from every individual or reliance another legal basis under Article 6 GDPR). Importantly however, organisations will be required: (i) to provide data subjects with an unconditional right to object to the processing of their personal data where such processing occurs; and (ii) implement appropriate **safeguards** which will include the **three-step test** to document and assess the necessity of the legitimate interest pursued by a controller or third party. See also EDPB Opinion 28/2024 on the use of personal data for the development and deployment of AI models (in respect of safeguards) (here and here).

GDPR Articles affected by the Proposal	Digital Omnibus on AI Proposal Reference	GDPR's Current Text	Omnibus Proposal Amendment (Emphasis added)	What is being changed?	What does this mean?
Article 9 (Processing of special categories of personal data	Articles 3(1)(a) and (b),	Article 9(2) provides a list of derogations from the general prohibition on the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.	*The following derogation is added to Article 9(2):* **"(k) processing in the context of the development and operation of an AI system... [as defined in the AI Act] ... or an AI model, subject to the conditions referred to in paragraph 5.** *The following Article 9(5) is added:* **"For processing referred to in point (k) of paragraph 2, appropriate organisational and technical measures shall be implemented to avoid the collection and otherwise processing of special categories of personal data. Where, despite the implementation of such measures, the controller identifies special categories of personal data in the datasets used for training, testing or validation or in the AI system or AI model, the controller shall remove such data. If removal of those data requires disproportionate effort, the controller shall in any event effectively protect without undue delay such data from being used to produce outputs, from being disclosed or otherwise made available to third parties."**	Introduces an additional derogation from the general prohibition on the processing of special categories of personal data for the residual processing of special categories of personal data for development and operation of an AI system or an AI model, subject to certain conditions set out; and	Identifies the circumstances in which limited processing of special categories of personal data may be carried out by controllers in an AI context. It provides a basis for controllers developing or deploying AI models or systems to use special category data for the development and operation of AI models and systems (subject to safeguards), without needing explicit consent from individuals (or relying on another exemption under Article 9 GDPR or national law). It also appears that this derogation acts as a carve out for right of erasure requests by including the following wording: "removal of those data requires disproportionate effort'. Clarification will also be required regarding the reference to "without undue delay" in this proposed new Article 9(5) GDPR.
Article 9 (Processing of special categories of personal data - biometric data)	Article 3(3)(a)	Article 9(2) provides a list of derogations from the general prohibition on the processing of personal data revealing ... biometric data for the purpose of uniquely identifying a natural person...	*The following derogation is added to Article 9(2):* **"(l) processing of biometric data is necessary for the purpose of confirming the identity of a data subject (verification), where the biometric data or the means needed for the verification is under the sole control of the data subject."**	Introduces an additional derogation from the general prohibition on the processing of special categories of personal data which concerns biometric data for the purpose of verifying the identity of an individual and the biometric data is under the control of the individual.	Identitfies the circumstances in which processing of biometric data may be processed for the purposes of identity verification where such data remain within the control of data subjects (i.e. on-device / remote facial recognition technology). This aligns with Annex III(1)(a) of

GDPR Articles affected by the Proposal	Digital Omnibus on AI Proposal Reference	GDPR's Current Text	Omnibus Proposal Amendment (Emphasis added)	What is being changed?	What does this mean?
					the EU AI Act concerning remote biometric identification systems such that the processing, and relevant AI system, are not considered 'high-risk'. This would prove very practical for addressing online impersonation and bot activity, and particularly useful in the digital services space (e.g. apps, online platforms, etc) as well as public services and financial services sectors.
Article 12(5) (Data Subject Rights Requests)	Article 3(3)(a)	"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, 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 the manifestly unfounded or excessive character of the request."	*The underlined text is added to Article 12(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.'**	Introduces a new exemption that data protection rights requests made by data subjects for purposes other than the protection of their data could be considered manifestly unfounded or excessive and therefore, permit a controller to refuse to respond to such requests.	Seeks to clarify when a controller may refuse to comply with data protection rights requests made by data subjects or charge reasonable fees. In particular, it calls out those circumstances where data subjects are making requests for reasons other than protecting their personal data (e.g. for collateral purposes, abuse of rights, litigation tactics, harassment, or negotiation leverage). While the burden of proof will remain with controllers to rely on this provision, it will be a welcome addition to the GDPR for many controllers, particulary in circumstances where data subject access requests are made in comtemplation of litigation or other out-of-court procedures. At a practical

GDPR Articles affected by the Proposal	Digital Omnibus on AI Proposal Reference	GDPR's Current Text	Omnibus Proposal Amendment (Emphasis added)	What is being changed?	What does this mean?
					level, the scope and impact of this exemption will require further clarification.
Article 13(4) (Information to be provided where personal data are collected from the data subject)	Article 3(5)	*Article 13 sets out information that controllers must provide data subjects when collecting personal data from them. Article 13(4) provides that:* "Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information."	*Article 13(4) is amended as follows:* "Paragraphs 1, 2 and 3 shall not apply where **the personal data have been collected in the context of a clear and circumscribed relationship between data subjects and a controller exercising an activity that is not data-intensive and there are reasonable grounds to assume that the data subject already has the information referred to in points (a) and (c) of paragraph 1, unless the controller transmits the data to other recipients or categories of recipients, transfers the data to a third country, carries out automated decision-making, including profiling, referred to in Article 22(1), or the processing is likely to result in a high risk to the rights and freedoms of data subjects within the meaning of Article 35."**	Removes the obligation to inform data subjects about the processing of their personal data in situations where there are reasonable grounds to assume that the data subject already has the information, **unless** the controller: (i) shares / discloses the relevant personal data to third party; (ii) transfers the data to a third country; or (iii) carries out automated decision-making or the processing is otherwise likely to cause a high risk to data subject rights and freedoms.	Reduces transparency obligations in respect of privacy notices for obvious, low-risk relationships (e.g., small businesses, associations). For example, there will be no requirement for a privacy notice where a controller directly collects personal data from an individual, and there are reasonable grounds to believe that the individual already knows the controller's identity, the purpose of processing the personal data, and how to contact any data protection officer. This reduced transparency obligation will not apply to personal data collected *indirectly* by controllers (i.e. Article 14 GDPR scenarios).
Article 22(1) and (2) (Automated individual decision-making, including profiling) (ADM)	Article 3(7)	"(1) The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. (2) Paragraph 1 shall not apply if the decision: (a) is necessary for entering into, or performance of, a contract	*Article 22(1) is amended as follows (and current Article 22(2) is replaced):* "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	Removes reference to ADM being a "prohibition" and expands the necessity for a contract legal basis such that a human is not required to make the ADM which produces legal effects or similarly significantly affects individuals.	This amendment will be relevant in an AI context and clarifies that ADM (with no human involvement) can be carried out when it is necessary for a contract, even if such decisions could be made by a human (i.e. manually).

GDPR Articles affected by the Proposal	Digital Omnibus on AI Proposal Reference	GDPR's Current Text	Omnibus Proposal Amendment (Emphasis added)	What is being changed?	What does this mean?
		between the data subject and a data controller; (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."	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."		
Article 33(1) (Notification of a personal data breach to the supervisory authority)	Article 3(8)	"In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay."	*Article 33(1) is amended as follows:* "In the case of a personal data breach **that is likely to result in a high risk to the rights and freedoms of natural persons,** the controller shall without undue delay and, where feasible, **not later than 96 hours after having become aware of it,** notify the personal data breach **via the single-entry point** established pursuant to... [the NIS 2 Directive] ...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." In addition: The European Data Protection Board (**EDPB**) must: (i) prepare a **"common notification template"** and **"a list of circumstances in which a breach is likely to result in a high risk to an individual's rights and freedoms"**; and (ii) review the template and **"at least every three years"** and "updated as necessary". *Importantly, and as alluded to above, the Digital Omnibus Proposal would also seek to make a change to the NIS 2 Directive (Directive (EU) 2022/2555), the Digital Operational Resilience Act (DORA) and the impending Critical Entities Resilience Directive to introduce a single-entry point for cybersecurity incident reporting. Such entry point would be established by ENISA (the European Union Agency for Cybersecurity). Until the single-entry*	Aligns the threshold for controllers to notify personal data breaches with the obligation to communicate with data subjects, i.e. the threshold in each instance will be high risk to the data subject's rights and freedoms. Extends the notification deadline by 24 hours, from 72 hours of a controller becoming aware about a breach to 96 hours of the controller becoming aware. Requires controllers to use a single-entry point notification portal (including where incident reporting is required under additional legal frameworks), yet to be established.	This will significantly reduce the burden of breach notification obligations, in particular the volume of notifiable personal data breaches made to data protection authorities since it increases the threshold that triggers such notification obligations from 'likely to result in a risk' to 'high risk'. This will also ensure that data protection authorities only receive notifications which have a potential or actual impact to the rights and freedoms of individuals. Provides organisations with an extra day (24 hours) to make notifications (where required) on becoming aware.

GDPR Articles affected by the Proposal	Digital Omnibus on AI Proposal Reference	GDPR's Current Text	Omnibus Proposal Amendment (Emphasis added)	What is being changed?	What does this mean?
			point is established, controllers would continue to notify personal data breaches directly to the competent supervisory authority. *There are related changes elsewhere in Article 33 to reflect this and which would also require the EDPB to prepare and submit a template breach notification to the Commission for adoption, along with 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.*	Reporting of breaches by processors to controllers is not addressed in the text.	Centralises reporting requirements across EU legislation, meaning controllers will only need to report once and relevant authorities will be notified subsequently. Further guidance will be required in respect of the information that will be required in breach notifications (i.e. the "template") along with the triggers for reporting such breaches (i.e. the "list"). This proposal will ultimately result in further alignment in breach notifications for controllers and remove existing inconsistencies of different information being required by the data protection authorities.
Article 35 (4), (5) and (6) (Data protection impact assessments) (DPIA)	Article 3(9)	"[...] 4. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68. 5. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment	"[...] 4. **The Board shall prepare** and transmit to the Commission a proposal for a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. 5. **The Board shall prepare** and transmit to the Commission a proposal for a list of the kind of processing operations for which no data protection impact assessment is required. 6. **The Board shall prepare and transmit to the Commission a proposal for a common template and a common methodology for conducting data protection impact assessments.**' [...]"	The EDPB would be required to prepare a single list of processing operations which require and do not require a data protection impact assessment, centralised at an EU level. Additionally, the EDPB would be obliged to prepare a proposal for a common template and common methodology for conducting data protection impact assessments.	Organisations will gain a better understanding of when a DPIA is required along with the requirements of the DPIA itself. Further guidance will be required in respect of the impact to existing guidance from the EDPB and data protection authorities.

GDPR Articles affected by the Proposal	Digital Omnibus on AI Proposal Reference	GDPR's Current Text	Omnibus Proposal Amendment (Emphasis added)	What is being changed?	What does this mean?
New Article 88a (Cookie trackers)	Article 3(15)	*No equivalent provision. This would be a* **new** *provision in the GDPR.* *Currently the legal regime on the processing of personal data on or from terminal equipment is regulated by the e-Privacy Directive (Directive 2002/58/EC).*	*A new Article 88a is inserted:* "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). 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) carrying out the transmission of an electronic communication over an electronic communications network; (b) providing a service explicitly requested by the data subject; (c) creating aggregated information about the usage of an online service to measure the audience of such a service, where it is carried out by the controller of that online service solely for its own use; (d) maintaining or restoring the security of a service provided by the controller and requested by the data subject or the terminal equipment used for the provision (e) of such service. 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) 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;**	Moves cookie rules from the e-Privacy Directive to the GDPR (incorporating into the GDPR the standard of consent for cookies where personal data are concerned). Existing e-Privacy rules for non-personal data will remain outside scope of the GDPR. Strengthens the choices available to individuals, requiring single-click buttons and mandatory time periods for "memory" of refusals. There are exemptions from cookie consent requirements, two of which apply where cookies are for the purposes of: (i) creating aggregated audience measurement for the controller's own use; or (ii) the security of the controller's service. In such instances, personal data collected under these exemptions can be processed subject to GDPR requirements	Simplifies the legal landscape and reduces "cookie banner fatigue" by requiring websites to have automated consent mechanisms (i.e. single click refusal mechanisms) and prohibiting such sites from re-requesting consent for the same purpose(s) within six months of the initial refusal or during any granted consent's validity period. Clarifies instances in which consent is not required for cookies. While it may consolidate compliance obligations and introduce harmonisation to cookies rules, it brings breaches of cookies rules to GDPR level penalties and will require new operational requirements from controllers to give effect to single-click consent preferences in addition to adhering to time periods prohibiting re-requesting cookie consent.

GDPR Articles affected by the Proposal	Digital Omnibus on AI Proposal Reference	GDPR's Current Text	Omnibus Proposal Amendment (Emphasis added)	What is being changed?	What does this mean?
			(b) if the data subject gives consent, the controller shall not make a new request for consent for the same purpose for the period during which the controller can lawfully rely on the consent of the data subject; **(c) if the data subject declines a request for consent, the controller shall not make a new request for consent for the same purpose for a period of at least six months.** This paragraph also applies to the subsequent processing of personal data based on consent. 5. This Article shall apply from [6 months following the date of entry into force of this Regulation].		
New Article 88b (Automated and machine-readable indications of data subject's choices with respect to processing of personal data in the terminal equipment of natural persons)	Article 3(15)	*No equivalent provision. This would be a* **new** *legislative provision in the GDPR. Currently the legal regime on the processing of personal data on or from terminal equipment is regulated by the e-Privacy Directive (Directive 2002/58/EC).*	*A new Article 88b is inserted:* "1. Controllers shall ensure that their online interfaces allow data subjects to: (a)Give consent through automated and machine-readable means, provided that the conditions for consent laid down in this Regulation are fulfilled; (b)decline a request for consent and exercise the right to object pursuant to Article 21(2) through automated and machine-readable means. [...] 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. [...]"	Codifies Court of Justice case law and EDPB guidance regarding the standard of consent for cookies (being the GDPR threshold of consent). Mandates respect for automated browser signals (like "Do Not Track" or newer standards) to refuse consent. Strengthens the choices available to individuals, requiring single-click buttons and mandatory time periods for "memory" for refusals. Implementation deadlines will be 24 months for controllers (who must enable the giving or refusal of consent via machine readable signals) and 48 months for browser providers (who must provide the technical means for users to transmit cookie consent preferences).	This may eventually eliminate cookie banners for users who set browser-level privacy preferences on websites (except media service providers such as online news / publishing sites - as defined in the EMFA). Standardisation in order to meet these requirements will be expected.

GDPR Articles affected by the Proposal	Digital Omnibus on AI Proposal Reference	GDPR's Current Text	Omnibus Proposal Amendment (Emphasis added)	What is being changed?	What does this mean?
				Media service providers (as defined the European Media Freedom Act (**EMFA**)) are exempted from adhering to consent signals given their reliance on digital ads revenues in upholding independent journalism.	

WILLIAM FRY

williamfry.com

DUBLIN | CORK | LONDON | NEW YORK | SAN FRANCISCO

William Fry LLP | T: +353 1 639 5000 | E: info@williamfry.com