INTERNET STIFTELSEN

The Swedish Internet Foundation's opinions on Simplification – digital package and omnibus – Proposal for a Regulation COM(2025)837

The Swedish Internet Foundation is an independent, private foundation that works for the positive development of the internet. We are responsible for the Swedish top-level domain .se and the operation of the top-level domain .nu, and our vision is that everyone in Sweden wants to, dares to and is able to use the internet.

Our opinions are limited to the proposals regarding GDPR and single entry point for incident reporting.

Summary

- The Swedish Internet Foundation supports the Commission's objective of simplifying compliance with the General Data Protection Regulation (GDPR), while maintaining a high level of protection of individuals' fundamental rights and freedoms and supporting EU competitiveness and innovation, including in artificial intelligence.
- The Swedish Internet Foundation emphasises that the GDPR constitutes a cornerstone of the protection of fundamental rights in the European Union. Any amendments should therefore meet strict requirements of necessity, proportionality and legal certainty.
- The Swedish Internet Foundation welcomes several elements of the proposal, including the extension of the deadline for personal data breach notifications from 72 to 96 hours and the development by the European Data Protection Board (EDPB) of guidance on Data Protection Impact Assessments (DPIAs).
- The Swedish Internet Foundation raises concerns regarding the proposed modification of the definition of personal data. The proposed approach, whereby data may be considered non-personal for an entity that cannot reasonably identify the individual concerned, would narrow the concept of personal data and may weaken the level of protection. It may also increase legal uncertainty as to what constitutes personal data. The Swedish Internet Foundation therefore encourages the Commission to maintain the current

definition and instead promote further guidance from the EDPB, including on issues such as pseudonymisation.

- The proposal also foresees the adoption of implementing acts concerning pseudonymised data. The Swedish Internet Foundation notes that detailed technical criteria risk becoming rapidly outdated and could, in practice, affect the material scope of the GDPR. A principles-based approach supported by guidance from the EDPB would be preferable to binding implementing acts.
- The proposal introduces an explicit reference to legitimate interests as a legal basis for processing in the development and operation of AI systems or models. The Swedish Internet Foundation considers that the existing framework under the GDPR already allows such processing where the conditions of Article 6(1)(f) are fulfilled. The introduction of a specific provision may therefore risk increasing complexity rather than providing additional clarity. The current case-by-case assessment should be maintained.
- The proposal further introduces an exception allowing incidental processing of special categories of personal data in the context of AI training and testing. The Swedish Internet Foundation is concerned that such an exception may reduce incentives to ensure careful control of training data. The Commission is therefore encouraged to reconsider the necessity of this exception. If retained, its scope should be clearly limited and the concept of “disproportionate effort” interpreted restrictively.
- The proposal also introduces a single entry point for incident reporting at EU level. While the Swedish Internet Foundation supports efforts to simplify reporting obligations, it considers that reporting should primarily take place at national level, with national authorities responsible for coordination and for forwarding relevant information to the EU level. Such an approach would better reflect national legal frameworks, supervisory mandates and confidentiality considerations, while avoiding the creation of an additional administrative layer.

1. Amendments to Regulation (EU) 2016/679 (GDPR)

1.1 Introduction

The Swedish Internet Foundation welcomes the Commission's objective to simplify compliance with regulations such as GDPR and strengthen individuals' ability to exercise their rights. We also recognise the Commission's objective to strengthen and stimulate EU competitiveness and enable innovation, including in artificial intelligence. However, we underline that the GDPR is a cornerstone of fundamental rights protection in the EU. Any adjustment must therefore meet a high bar for necessity, proportionality, and legal certainty to ensure a high level of protection of individuals' fundamental rights and freedoms.

The Swedish Internet Foundation welcomes several of the Commission's suggested changes to the GDPR. We welcome the extended deadline for personal data breach notifications, from 72 to 96 hours, since the current deadline may be challenging as it can include weekends and bank holidays which may be particularly challenging for small organisations. The extended deadline could also lead to supervisory authorities receiving more complete and accurate information, and remediation measures potentially implemented even before the breach notification.

The Swedish Internet Foundation also welcomes the development by the EDPB of lists of processing that do and do not require a Data Protection Impact Assessment (DPIA) and a DPIA template and methodology. These initiatives would bring more clarity and hopefully strengthen the protection of individuals' fundamental rights and freedoms.

However, we do express significant concerns regarding some of the proposed changes, for example the proposed changes to the definition of personal data.

We limit our response to detailed comments on the proposed changes set out in the sections below.

1.2 Changes to the definition of personal data

The Commission's proposal aims to clarify that information should not be regarded as personal data "for a given entity" if that entity does not have means "reasonably likely" to be used to identify the individual. Modifying the definition of personal data would directly impact the material scope of the GDPR.

The Swedish Internet Foundation fully agrees with the EDPB-EDPS Joint Opinion[1], which states that "the proposed changes to the definition of personal data would narrow the concept of personal data and would adversely affect the fundamental right to data protection. The proposed changes go far beyond a targeted modification of the GDPR, a 'technical amendment' or a mere codification of CJEU jurisprudence."[2]

We further consider that the suggested changes would not result in legal certainty but rather increase uncertainty as to what constitutes personal data. The proposed changes could also increase the risk of organisations attemting to circumvent the data protection legislation.

A more in-depth impact assessment of the potential adverse consequences of the proposed changes would have been welcome, including their implication for the protection of individuals' fundamental rights and freedoms.

We therefore encourage the Commission not to adopt the proposed changes to the definition of personal data. To cite the EDPB-EDPS Joint Opinion: "[…] the definition should say what personal data is, instead of what it is not."[3]

Instead of amending the definition of personal data under the GDPR, we welcome further clarification and guidance from the EDPB on complex issues, such as pseudonymisation, taking recent developments and judgments (e.g. EDPS v SRB judgment[4]) into consideration.

This is particularly relevant considering the Commission´s proposed introduction of new implementing acts related to pseudonymisation, see below.

1.3 Implementing acts to clarify whether data resulting from pseudonymisation constitutes personal data for certain entities

The proposed new Article 41a of the GDPR would empower the Commission to adopt implementing acts to specify means and criteria – not only legal but also technical – to determine whether data resulting from pseudonymisation no longer

[1] EDPB-EDPS JOINT OPINION 2/2026 On the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus), adopted on 10 February 2026.
[2] EDPB-EDPS JOINT OPINION 2/2026 On the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus), adopted on 10 February 2026, page 4.
[3] EDPB-EDPS JOINT OPINION 2/2026 On the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus), adopted on 10 February 2026, page 10.
[4] EDPS v SRB, CJEU judgment Case C-413/23 P.

constitutes personal data for certain entities. This amendment would complement the proposed change to the definition of personal data.

The Swedish Internet Foundation raises concerns that overly detailed technical criteria for assessing when data is considered pseudonymised may quickly become outdated and irrelevant. Since the implementing acts would be binding, organisations could be required to use technical implementations that might not be the most appropriate with current technical or privacy standards. We encourage a more principles-based approach supplemented by practical examples. As noted above, we would welcome the EDPB to address these issues through guidance rather than through an implementing act.

An implementing act, as proposed, could also greatly affect the material scope of the GDPR, changing the scope of when and for whom information is considered personal data. We agree with the EDPB-EDPS Joint Opinion, which states "[…] that defining what is no longer personal data should not be addressed in an implementing act and that it should be the competence of supervisory authorities, under the control of the competent courts, to apply the definitions of the GDPR in an independent manner […] and it is the competence of the EDPB to ensure consistent application on this matter." [5]

1.4 Use of legitimate interest in the context of an AI system or model

The proposed new Article 88c states that processing in the context of development and operation of AI systems or models may be pursued for legitimate interests. The Swedish Internet Foundation considers that it is already clear, according to the GDPR, where the conditions in Article 6(1)(f) of the GDPR are met, legitimate interests can, in certain cases, serve as a lawful basis for processing carried out in connection with the development and deployment of AI systems or models. This has also been concluded by the EDPB in its Opinion 28/2024 on AI models[6].

[5] EDPB-EDPS JOINT OPINION 2/2026 On the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus), adopted on 10 February 2026, page 12.
[6] EDPB Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models, adopted on 17 December 2024, Section 3.3

We question whether a specific provision is necessary in the GDPR to state that legitimate interest may serve as a lawful basis in this context, as it might risk adding complexity rather than clarity.

An explicit reference to AI-related processing as a context in which controllers may rely on the legitimate interest could also be understood as a signal that the legitimate interest assessment can be less thorough, simply because the legislator has already identified the context as “legitimate”. We consider it preferable to maintain the current legislation, whereby the applicability of Article 6(1)(f) is not predetermined for specific purposes or contexts of processing but is assessed on a case-by-case basis through a thorough and documented legitimate interest assessment, conducted in accordance with EDPB guidance[7].

1.5 Additional exemption for incidental and residual processing of special categories of personal data in the context of the development and operation of an AI system or model

The Commission proposal introduces an additional exception from the general prohibition on processing special categories of personal data by adding a new point (k) in Article 9(2) GDPR, covering “processing in the context of the development and operation of an AI system […] or an AI model”, subject to specific conditions set out in a new Article 9(5). The proposed Recital 33 explains the rationale as addressing scenarios where special categories of personal data “may residually exist” in training, testing or validation datasets, or be retained in an AI system or AI model, even though such data are not necessary for the purpose of the processing.

The Swedish Internet Foundation recognises the Commission’s objective to strengthen and stimulate EU competitiveness and enable innovation, including in artificial intelligence. However, we question the introduction of a broad AI-specific exception in Article 9(2) GDPR for situations where special categories of personal data are not necessary for the processing purpose, but are incidentally included. We are concerned that the proposed exception could result in organisations showing less concern about what personal data, even special categories of personal data, are used for training and testing and retained in an AI system or model.

[7] EDPB Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, adopted on 8 October 2024.

We also have concerns regarding the introduction and practical application of the "disproportionate effort" threshold for removal. The proposed Recital 33 indicates that if removal of residual special categories of personal data in an AI system or model would require re-engineering or retraining the system or model, this is deemed a "disproportionate effort". It would be problematic if re-engineering or retraining efforts were characterised as "disproportionate", rather than treated as a necessary remedial measure to restore compliance and reduce risks for data subjects.

We therefore encourage the Commission to reconsider whether an additional, AI-specific exception under Article 9(2) GDPR is necessary or proportionate, given the central role of Article 9 in safeguarding individuals' personal data that is considered particularly sensitive such as health data.

If the exception is nevertheless maintained, it should be narrowed and clarified that "disproportionate effort" should be interpreted restrictively, and that the exception only applies where controllers can demonstrate that the presence of special categories is genuinely incidental and unavoidable despite effective preventive measures.

2. Single entry point for incident reporting

It is proposed that ENISA should develop and maintain a common contact point to facilitate compliance with the obligation to report incidents and related events under the Union legal acts in which such reporting is required.

The Swedish Internet Foundation is, in principle, positive towards a model based on a single entry point for incident reporting. However, in accordance with the principle of subsidiarity, such a function should not take the form of an EU-level central recipient as the first point of contact.

Instead, we advocate national reporting as the primary channel, followed by EU-level coordination at an aggregated level, under which national authorities would forward relevant information to the EU level (for example, to ENISA).

Such a model would provide better conditions for accurate assessment and handling in light of the national context, including applicable mandates, legislation, and legal traditions. National authorities already have established roles and responsibilities and—crucially—the legal mandate to take supervisory measures and impose

sanctions. Member States also differ in key areas such as freedom of expression and access to public information, which further supports the case for national first-line reporting.

The approach also raises certain questions regarding confidentiality and national security if incident reports were to be collected by a centralised European body.

Should the EU level nevertheless become the primary entry point for reporting, we consider it essential that each Member State designate a clearly identified national function within this structure, responsible for initially acting as incident manager and for handling national coordination and communication. Such a model already exists within other EU cooperation frameworks, for example Europol, and could similarly be applied in this context.

In summary, we assess that EU-level primary reporting risks creating an additional administrative layer rather than a genuine simplification, particularly for actors whose operations are primarily national. At the same time, we recognise that cross-border actors may favour a different arrangement for reasons related to equal treatment and efficiency.

The Swedish Internet Foundation therefore recommends national reporting as the first step, followed by EU-level coordination at an aggregated level through the responsible national authorities.

3. In addition, we support the position expressed in the CENTR Board Statement on the Digital Package (Digital Omnibus).

CENTR (the Council of European National Top-Level Domain Registries) represents the operators of European country-code top-level domains (ccTLDs), including national domain registries such as .se, .de and .fr. As an industry association representing the operational perspective of European ccTLD registries, CENTR provides expertise on the practical implications of EU digital regulation for critical internet infrastructure.

As outlined in the CENTR statement, the current EU regulatory landscape risks creating unnecessary complexity by duplicating audits, supervisory powers and

baseline cyber risk-management requirements across several legislative instruments. Such duplication does not add value and should be simplified and clarified.

Conformity checks for the same legislative requirements should therefore be limited to a single audit per operator under the main cybersecurity legislation.

In addition, the European Commission and Member States should support the establishment of a single, secure national reporting interface in each Member State, in order to streamline incident reporting and reduce unnecessary administrative burden.

Finally, the European Commission should assess overlaps across legislative instruments and ensure that essential entities are not required to report the same incident under multiple regulatory frameworks.

Reference: CENTR Board Statement on the Digital Package (Digital Omnibus)

https://www.centr.org/news/news/centr-issues-board-statement-on-digital-package-digital-omnibus.html

2026-03-12

Carl Piva, CEO

The Swedish Internet Foundation