Council of the European Union
General Secretariat

Interinstitutional files:
2025/0360 (COD)

Brussels, 04 June 2026

WK 7876/2026 ADD 1

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:	Omnibus VII (Digital): Written comments/suggestions from Member States on Presidency revised compromise text (P2B, GDPR, e-privacy/cookies, cyber)

Delegations will find attached the comments on the Presidency revised compromise text (deadline 02 June 2026) from the following Member States: HR and RO.

CROATIA – comments to the third compromise text
(Omnibus VII - GDPR+ cookies +e-Privacy)

General remarks

In principle, Croatia supports the objective of the proposal to make the European Union's digital regulatory framework clearer, more enforceable and less administratively burdensome for entrepreneurs, public authorities and citizens. It is evident that micro, small practices and medium-sized enterprises in particular have difficulties in understanding and applying the obligations under the GDPR, and the further complexity of the digital regulatory framework further complicates compliance.

However, personal simplification cannot lead to a reduction in the level of data, weakening of patients' rights or reducing the possibility of effective supervision. It is particularly important to maintain the logic of the GDPR according to which compliance is not based only on the formal fulfillment of obligations, but on the principles of lawfulness, fairness, transparency, data minimization, security and reliability of the processing.

The proposed amendments can be useful if they bring real legal clarity, in particular in the areas of pseudonymization, impact assessment, reporting of breaches and the use of personal data in the context of AI systems. However, the specific solution needs to be further clarified and limited in order to avoid misinterpretations in practice.

Pseudonymisation and the definition of personal data

Croatia welcomes the effort to further clarify the relationship between pseudonymisation and the notion of personal data. In practice, there is often uncertainty about when pseudonymised data still constitutes personal data, in particular in the context of data transfers to third parties, scientific research, the development of AI models and the processing of large data sets.

It is positive that the compromise text emphasises that identifiability must be assessed with regard to means that are reasonably likely to be used for the specific controller, processor or recipient of the data. Such an approach is in line with the case-law of the Court of Justice of the EU and it can contribute to greater legal certainty. However, it is necessary to avoid an interpretation according to which pseudonymisation would automatically lead to an exit from the scope of the GDPR. Pseudonymisation is an important security measure, but it is not the same as anonymisation. It is therefore useful to maintain the emphasis that the controller and processor remain responsible for assessing the risk of re-identification and for proving that the specific data for a specific recipient no longer allow the identification of the data subject.

Croatia upports strengthening the role of the EDPB in drafting opinions on pseudonymisation and anonymisation. Such opinions should be practical, technically sound and regularly updated, with public consultation with relevant stakeholders. It is particularly important that the opinion addresses scenarios for the use of pseudonymised data in AI development, research, healthcare, the public sector and data transfers between multiple actors.

HR proposal:

Retain the clarification that pseudonymised data does not have to be personal data for each recipient, but explicitly emphasise that such an assessment must be specific, documented, technically and organisationally sound and subject to supervision.

Use of personal data for the development and operation of AI systems based on legitimate interest

Croatia welcomes the effort to clarify the possible use of legitimate interest as a legal basis for the processing of personal data in the context of the development and operation of AI systems or AI models. In practice, this is one of the most important and sensitive issues, as the development of AI systems often involves large amounts of data, secondary use of data, web scraping, model validation, testing, optimization and security checks.
However, it is necessary to avoid the interpretation that legitimate interest is the "default" or preferred legal basis for the development of AI systems. Each processing must continue to be assessed individually. The controller must demonstrate the existence of a legitimate interest, the necessity of the processing and the overriding of that interest over the rights and freedoms of the data subjects.
It is particularly important to maintain the conditions set out in the compromise text: increased transparency, unconditional right to object, respect for technical signals limiting the use of data for AI development, the application of privacy-preserving techniques, data reduction and measures against regurgitation, data leakage and other foreseeable risks.

Namely, it is particularly important to clearly distinguish the following situations:
- development of AI models,
- testing and validation of AI models,
- use/deployment of AI systems in a specific business process,
- processing of data entered by users in prompts,
- processing of special categories of data,
- processing of children's data,
- automated decision-making that produces legal or similar significant effects.

These situations do not have the same level of risk and cannot be treated equally.

HR proposal:
The text should further emphasize that the possibility of relying on legitimate interest in the AI context should not be interpreted as a general permission for the processing of personal data for the development or operation of AI systems. The requirement for a legitimate interest test, enhanced transparency, the right to object and documentation of the assessment carried out should be explicitly retained.

Incidental and residual processing of special categories of personal data in the AI context

The proposed exception in Article 9 should not lead to the normalization of the processing of special categories of data in AI systems. It must remain narrow, exceptional and strictly conditional. It is particularly important to clearly distinguish the situation in which special categories of data appear incidentally and residually from the situation in which the controller intentionally uses such data for the development or use of AI systems.
It is positive that the text provides for the obligation of technical and organizational measures to avoid such processing, the removal of special categories of data when they are identified,

protection from further processing if removal is not possible, the documentation and regular review of the effectiveness of the measures.

However, it is necessary to further clarify what is meant by "manifestly disproportionate effort" in the context of the impossibility of erasing such data. Otherwise, there is a risk that controllers will make too broad use of this exception.

Our proposal:
Retain the exception only for truly incidental and residual processing of special categories of data, subject to documented assessment, periodic review, clear demarcation from intentional processing, and a strict prohibition on the use of such data for output generation, profiling, or further disclosure to third parties.

Informing data subjects according to Article 13 of the GDPR

Croatia understands the objective of reducing the administrative burden in situations of clear, simple and low-risk relationships between controllers and data subjects, for example in the case of craftsmen, smaller service providers, associations.
However, the exception to the information obligation must remain very narrow. The right to information is the basis of transparency and a prerequisite for the exercise of other rights of data subjects. If the data subject is not clearly informed about the processing, it is difficult for him to exercise the right of access, rectification, erasure, objection or restriction of processing.
It is positive that the compromise text excludes the application of this exception in cases of data transfer to third parties, transfer to third countries, automated decision-making, including profiling, and high-risk processing. This limitation should be maintained.
In particular, we emphasize that this exception should not apply in the context of the use of AI tools, profiling, processing of employee data, public bodies, processing of special categories of data or any processing that is not simple, foreseeable and low-risk.

HR proposal:
Further clarify that the exception in Article 13, paragraph 4, does not cover AI uses, profiling, processing of employee data, processing of special categories of data, public sector or more complex digital processing. It is recommended to maintain at least a minimum obligation to provide basic information about the controller, the purpose and the rights of the data subject.

Automated decision-making and Article 22 of the GDPR

Croatia believes that the amendments to Article 22 must be viewed with great caution. Article 22 is one of the key mechanisms for protecting data subjects in the context of automated decision-making, profiling and AI systems that can have legal or similar significant effects on individuals.
The proposed clarification that a decision may be necessary for the conclusion or performance of a contract even if it could technically be made by a human being may contribute to legal clarity. However, there is a risk that this formulation will be interpreted too broadly in practice and that automated decision-making will be normalised in situations where it is not really necessary.
We point out that necessity must not only mean business convenience, cost reduction or organisational efficiency. There must be a real need for the automated decision in a specific context, with clear safeguards.

It is particularly important to maintain the right to human intervention, the right to express a point of view and the right to challenge the decision. Human intervention must not be formal, but real and effective. The person carrying out the intervention must have the authority, knowledge and possibility to change the decision.

HR proposal:
Further clarify that the "necessity" of an automated decision does not only encompass business efficiency or cost reduction and that Article 22 must be interpreted in accordance with the principles of fairness, transparency, data minimisation and effective human intervention.

Data protection by design and by default for processors

Croatia welcomes the proposal to more clearly extend the obligations of technical and integrated data protection to processors, in the part relating to their own obligations. In practice, processors, in particular providers of cloud services, SaaS solutions, AI tools and technical infrastructure, often play a key role in whether the controller can implement GDPR compliance at all. This is particularly important in the context of AI systems. The controller often uses a ready-made tool or platform and does not have full control over the technical architecture, security settings, location of processing, logging, data retention, possibility of deletion or the way in which user data is used. It is positive that the text retains the controller's responsibility for determining the purposes and means of processing, but at the same time recognises that the processor must offer services that enable technical and integrated data protection.

HR proposal:
Retain this amendment, but further clarify that implementers, especially AI and cloud service providers, must design their services in a way that enables controllers to meet GDPR obligations, including data reduction, security, access control, deletion, storage limitation, transparency and documentation.

Personal data breach reporting

Croatia expresses serious reservations regarding the proposal to align the threshold for reporting a personal data breach to the supervisory authority with the threshold for notifying data subjects, i.e., requiring reporting to the supervisory authority only when it is likely that the breach will result in a high risk to the rights and freedoms of individuals. Such a change could significantly reduce the number of reports to supervisory authorities, but could also weaken the preventive and supervisory function of the breach reporting system. In the Croatian context, the number of reports is already extremely low, around 100 reports per year, and in the EU context, we are in second to last place in this regard.

Through breach reports, supervisory authorities monitor not only individual high-risk cases, but also patterns of security breaches, recurring vulnerabilities, sectoral risks, the behavior of the processor and the level of organizational maturity of the controller.
If the controller independently incorrectly assesses that the breach is not high-risk, the supervisory authority may never learn about it. This is particularly problematic for smaller organizations that do not have developed risk assessment capacities.

We support the harmonisation of templates and the development of a common list of circumstances in which a breach is likely to be high-risk or not. However, such tools should not replace the obligation to report appropriately to the supervisory authority.

HR proposal:
Maintain the existing threshold for reporting to the supervisory authority or, if the threshold is changed, introduce additional safeguards: an obligation to document all breaches in detail internally, the possibility of ex post verification by the supervisory authority, a clear EU list of high-risk and low-risk breaches, and an obligation to periodically report or make records of breaches available upon request by the supervisory authority.

Contact details of the data protection officer

Croatia does not support the abolition of the obligation to provide the contact details of the data protection officer to the supervisory authority. The proposed amendment to Article 37, paragraph 7, according to which the controller or processor would only publish the contact details of the DPO, without the obligation to communicate this data to the supervisory authority, may make the work of the supervisory authorities more difficult.
In practice, the contact details of the data protection officer enable the supervisory authority to communicate quickly with organisations, deal with complaints more effectively, provide advice, carry out targeted training and crisis communication in the event of personal data breaches or other urgent situations.
For the supervisory authority, up-to-date contacts of the DPO are an important operational tool. For example, every year we carry out control checks, supervisory actions via questionnaires that we send to the addresses of the data protection officer as the person responsible for compliance with data protection legislation in the organisation.

HR proposal:
Retain the existing obligation for the controller and processor to publish the contact details of the DPO and submit them to the supervisory authority

Excessive or abusive requests from data subjects and complaints to supervisory authorities

Croatia understands the need to protect controllers and supervisory authorities from manifestly abusive, repetitive or instrumental requests. In practice, there are situations where the right of access or the right to complain is used for purposes not related to the protection of personal data. However, this exception must remain strictly limited. The rights of data subjects and the right to complain to a supervisory authority are a fundamental mechanism for implementing the GDPR. Unclear or overly broad wording could deter data subjects from exercising their rights or allow controllers to unjustifiably reject requests.
We support keeping the burden of proof on the controller or supervisory authority. It is also important to clearly distinguish between repetitive requests that are justified and genuinely abusive requests.

National entry point for reporting incidents

Croatia supports the idea of simplifying multiple reporting obligations on incidents. In practice, the same event may trigger several different obligations under the GDPR, NIS2, DORA, eIDAS

or other regulations. This can be complex for organisations and operationally demanding for authorities. However, a national entry point must not diminish the independence, competences and timely access to information of data protection supervisory authorities. Reporting a personal data breach under the GDPR has a specific purpose: to protect the rights and freedoms of natural persons. This purpose must not be lost in the broader cyber-incident reporting framework.

It is necessary to ensure that the data protection supervisory authority receives all relevant information without delay, in a format that allows for effective assessment and action. It is also important that the establishment of a national entry point does not delay the start of the period for reporting a breach or create ambiguity as to when a report is deemed to have been submitted.

HR proposal:
Support national entry points, but with clear safeguards: timely transmission to the DPA, preservation of confidentiality, security measures, clear rules on deadlines, preservation of the independence of supervisory authorities and the possibility for the DPA to communicate directly with the controller when necessary

Additional comments from Romania

Romania express support for the opinion presented by Italy and Sweden at the meeting of the AGS on the 8th of May 2026, according to which DORA should be considered a reference point ("benchmark") for the incident notification system (in accordance with the NIS2 Directive), for which we consider that it would be useful to establish several entry-points at national level (according to the competences of national authorities in their respective fields of responsibility), which would cooperate with each other.

Additionally, Romania supports the proposals presented in Poland's non-paper on cookies.