UNITED NATIONS HUMAN RIGHTS OFFICE OF THE HIGH COMMISSIONER | Representation Office to the European Union

REFLECTIONS ON THE INTERNATIONAL DIMENSIONS OF THE EU DIGITAL OMNIBUS

EXPERT ROUNDTABLE
18 MAY 2026, IN BRUSSELS AND ONLINE

SUMMARY NOTES

In the presence of

Christina Meinecke
Regional Representative, Office of the UN High Commissioner for Human Rights (OHCHR)

Prof. Lyra Jakulevičienė
Member of the UN Working Group on Business and Human Rights

BACKGROUND

The Office of the United Nations High Commissioner for Human Rights (OHCHR/UN Human Rights) is the leading UN entity on human rights. UN Human Rights is mandated to speak out objectively when human rights violations occur and to help develop the standards used to evaluate human rights progress worldwide. Under the United Nations Global Digital Compact, UN Human Rights is to provide advisory services to stakeholders to align governance and regulation of digital technologies with international human rights norms and standards.

Published in November 2025, the European Commission's proposed a Regulation on Simplification of digital legislation (the Digital Omnibus) which suggests changes to the EU's General Data Protection Regulation (GDPR), the Regulation 2024/1689 (EU's AI Act), and the Directive 2002/58/EC (e-privacy Directive[1]). The GDPR has frequently been referred to as "the most comprehensive model for protecting the right to privacy" in the digital age, on account of its right-based approach. The E-privacy Directive is also significant in that it clearly codifies the right to communicate securely, a right which is crucial in a democracy as it also enables the enjoyment of other rights such as freedom of expression and association. Although there are some shortcomings, the EU's AI Act provides an important framework to bring more transparency and accountability to the use of AI and includes important human rights protections, some of which are now also being reopened.

In general, European Union (EU) legislation has a significant global influence on norms. In this context, UN Human Rights convened an expert roundtable to examine the proposed changes and their potential impact on human rights protection, particularly in other regions which may draw on EU legislation for guidance. The event took place in person and online on 18 May 2026. There were over 100 participants, including representatives of the European Union institutions, international and non-governmental organizations, data protection authorities, equality bodies, academics, civil society organizations, and the European Network of National Human Rights Institutions.

Below is a summary note of the expert-level roundtable without attributions which was held under the Chatham House Rule.

SUMMARY NOTE

1. **Avoid fragmentation between overlapping due diligence obligations, since this would complicate rather than simplify compliance for businesses.**

Participants noted that due diligence obligations for businesses exist beyond EU law. They stem from requirements of investors, contractual clauses, supply chain management, and the practices under the UN Guiding Principles on Business and Human Rights. The risk of human rights violations due to the use of AI systems do not disappear if obligations are reduced. Reduction of the scope of obligations under the Digital Omnibus in the EU law could create a parallel system of legal expectations that would complicate rather than simplify business implementation of human rights obligations.

2. **Ground EU digital governance firmly in international human rights law, as committed to under the UN Global Digital Compact and given the EU's influence as a global standard-setter.**

Participants noted that digital governance decisions taken by the EU have effects far beyond its borders. Because EU rules are widely "copied", adapted, and invoked around the world, reforms proposed in the EU Digital Omnibus should be assessed not only for their impact within the EU, but also for how they may influence legal protection and enforcement practices globally. It was also noted that whilst some countries outside the EU align with EU regulations, this does not always translate into alignment with international human rights law. There is a risk of selective replication or "cherry picking," where restrictive or permissive provisions are copied without corresponding oversight and accountability mechanisms. This, it was argued, makes it particularly important to preserve strong safeguards in EU digital law reforms.

3. **Welcome privacy signals as useful contribution to global digital governance but clear legal definition needed.**

Properly designed privacy signals could make a valuable contribution to global digital governance by making it easier for people to refuse, object, and withdraw consent. This will work only if their legal meaning is clearly defined in law, applied consistently across browsers, operating systems, applications, and software development kit-based environments, and designed not to create new layers of tracking. If their meaning is left mainly to technical standard-setting processes, there is a real risk that the industry will ultimately shape the practical meaning of people's rights.

4. **Maintain the current definition of personal data and avoid expanding lawful bases for AI training in ways that weaken purpose limitation, data minimization, and effective user control.**

The GDPR has served as a global model, with an estimated 160 data protection frameworks incorporating its principles. Participants at the roundtable expressed reservation about the proposal to redefine and narrow the definition of personal data, as this would enable a subjective classification of what constitutes personal data and lead to a relative protection of individuals' personal data. Because the definition of personal data underpins the material scope of the legislation, any change to that definition would affect how the legislation applies.

It was considered that if the EU followed through with such an approach, other countries may follow suit, leading to a general erosion of data protection norms worldwide. This perspective highlighted the EU's role as a regulatory leader and the potential consequences of altering its framework. The change in definition could also lead to the exclusion of certain data sets, such as pseudonymized data, from GDPR protections.

As the definition of pseudonymization is not precise and relational, legal certainty about what is protected subject matter and what is not, would erode. It was noted that as an existing barrier to enforcement that some entities engage in "malicious compliance" by exploiting legal ambiguities and prolonging litigation. Concern was raised that this problem could be further exacerbated by the proposed change allowing controllers to subjectively decide whether information qualifies as personal data. This could heighten legal uncertainty and open the door to further exploitation of ambiguity.

5. **Ensure that international human rights law guides cross-border cooperation on cybercrime and avoid reforms that weaken safeguards for international data transfers or increase risk of transnational repression.**

States are increasingly relying on each other to investigate, request data, and pursue accountability, including through mutual legal assistance and wider international cooperation, especially in the context of the new UN Convention on Cybercrime. That cooperation must be built on a clear human rights foundation. Cybercrime is inherently cross border, and the associated risks of transnational repression are real.

That is why the UN human rights framework should guide national action, and why robust safeguards must underpin any cross-border exchange of information and evidence. This is very relevant in the context of the Digital Omnibus debate on GDPR because the changes in definition of personal data could mean that the EU privacy rules may stop applying at the point of export.[2] That can mean the usual safeguards for sending data overseas do not apply, which is especially concerning when data is shared with international organizations, including law enforcement bodies.

Weakening the definition of personal data could remove certain international transfers from the GDPR's scope altogether, meaning Chapter V safeguards would no longer apply in practice. This is especially significant for transfers to third countries and international organizations, including in law enforcement contexts, where robust human rights safeguards remain essential. The proposed changes to the e-privacy Directive could further weaken overall safeguards given that it would decrease device-level privacy protections.

6. **Apply a strict human rights and proportionality approach to any derogations for processing sensitive data in AI development, to prevent discriminatory outcomes.**

Digital Omnibus proposes to allow for derogations against the prohibition on processing sensitive data in the context of the development of certain AI systems. Participants stressed how AI systems can perpetuate discrimination, and how proxy-based discrimination emerges as a central risk as AI can infer protected traits, creating systemic indirect discrimination. Participants expressed concern that the challenge of discrimination has not been robustly considered in the proposed text. Allowing for processing of sensitive personal data, combined with the broader definition of personal data would appear to increase, not diminish the risk of direct and indirect discriminatory outputs.

The notion that sensitive personal data may remain in AI training sets based on companies' claim that to remove it would be too difficult should be challenged. Allowing the processing of special categories of personal data for AI development where controllers claim it is too difficult to identify or remove such data, creates significant human rights risks.

Combined with broader personal data rules, these exceptions could heighten risks of direct and indirect discrimination, including proxy-based discrimination in AI systems. Broadening "legitimate interest" for AI training could allow data to be reused for purposes for which it was not originally collected, without a sufficiently specific objective or proportionality assessment.

7. **Preserve transparency, access, and contestation rights as core accountability tools in AI-related data processing and decision-making.**

Participants expressed concern that the proposed changes to data subject rights would expand exemptions to transparency and access to information rights which would further weaken the rights of data subjects and could result in people being unable to assess or challenge automated outcomes. This would impair data subject's access to explanation and contestation and undermine therefore the right to an effective remedy under international human rights law including the UN Guiding Principles on Business and Human Rights, which also apply to business use of AI. It was noted that the right to scrutinize and challenge the processing of personal data goes beyond the question of data protection, as the GDPR protects all fundamental rights (Art. 1(2)).

Furthermore, weakening transparency obligations such as model provenance, dataset disclosure, and access rights would make it harder for people to understand how their data is used and to challenge automated/AI-powered decision making.

8. **Welcome continued mandatory public reporting on whether AI systems are high-risk, while recognizing that stronger practical accountability measures are still needed.**

Participants noted that the political agreement on the amended AI Act text had maintained the transparency requirement on companies to publish their self-assessments on whether their AI systems fall into a high-risk category. It was noted that the provision was nevertheless weakened given that companies would have to provide less information. This is a practice which would have to be carefully monitored, going forward to examine its effectiveness.

9. **Safeguard the powers and resources of Article 77 Fundamental Rights Authorities and preserve meaningful access to information for independent oversight.**

Accountability actors such as Article 77 entities, including National Human Rights Institutions and equality bodies, need effective access to information to investigate and challenge harms. Participants noted that the Digital Omnibus proposes to reduce powers for Article 77 entities to request information directly which would leave them with greater dependence on market surveillance authorities and undefined 'reasoned request' standards. Amendments that would limit Article 77 entities' ability to fulfil their role meaningfully would require them to obtain information only through market surveillance authorities (MSAs), creating risks of delay, information filtering, and dependence on MSA capacity, while also subjecting them to undefined 'reasoned request' requirements that create legal uncertainty.

10. **Strengthen structured dialogue between Article 77 entities and civil society so each can benefit from the other's expertise and capacities.**

A useful exchange between civil society actors and Art. 77 entities during the roundtable led to discussions exploring how the relationship could be further developed given the high potential of mutual complementarity. Civil society actors have deep-expertise which can complement the Art. 77 entities access information and transparency powers.

11. **Undertake a full human rights impact assessment of the Digital Omnibus.**

Well-organized participation is key to help ensure evidence-based policymaking in time-sensitive situations. The international impact of this Digital Omnibus should also be considered in terms of the potential of other governments using 'technical simplification' to amend legislation without a comprehensive and participatory approach on the human rights impact.

---

1. Note that participants referred to both the E-privacy Regulation and the Directive, the former still not being in force but nevertheless impacted by the current debate.
2. Linked to the proposed changes to personal data under the EU Digital Omnibus and GDPR Art. 44-50 and Recital 41