Open letter to the Council of the European Union: do not let digital simplification become deregulation

To the Cypriot Presidency of the Council of the European Union and the Permanent Representations of the Member States,

We, the undersigned civil society organisations, are writing to you regarding the Council's work on the Proposal for a Regulation as regards the simplification of the digital legislative framework, known as the Digital Omnibus, and in particular its GDPR and ePrivacy aspects (the so-called 'Data Omnibus')[1]. While this file is presented as a simplification exercise, several parts of the Commission proposal related to the GDPR and ePrivacy go far beyond mere simplification of rules. These parts would weaken core safeguards, reduce legal certainty, and lower the practical protection of fundamental rights. The GDPR and ePrivacy are not administrative burdens. They are central pillars of a rights-based European digital rulebook. They protect people against intrusive tracking, unlawful data use, opaque profiling, and abusive automation. They also give responsible organisations the legal certainty they need.

Moreover, the process of developing the Digital Omnibus is also problematic. Any package that changes how fundamental rights are protected in a digital environment should be supported by evidence, comply with the EU's Better Regulation standards, and include a proper fundamental rights impact assessment across the whole proposal. With this in mind, we welcomed the Council's earlier efforts to remove or narrow some of the most harmful elements of the Commission's proposal, although recent developments suggest these may now be reversed. The protective direction must be preserved or reinstated where it has been weakened.

The Council should maintain the deletion of GDPR-related proposals that have weakened the definition of personal data, created broad openings for AI-related processing or reduced key safeguards for people. Taken together, these proposals would move the GDPR away from enforceable rights and towards more controller discretion, more Commission-led reinterpretation of core concepts, and more responsibility placed on people to protect themselves against systems they cannot see or meaningfully contest. Reopening the GDPR's core architecture through the Omnibus would create more uncertainty, more litigation, and weaker rights.

Deleted proposals should not in any way return through the back door. Recitals, guidance mandates, standards, and vague compromise language can have real legal effects in practice. They should not be used to revive risky ideas on AI-related processing, pseudonymisation, identifiability, scientific research, or legitimate interest, after the operative provisions have been removed.

We welcome the fact that the current Council compromise apparently keeps the rules on access to terminal equipment within the ePrivacy framework, rather than transferring them into the GDPR. This direction must be preserved. The GDPR governs the processing of personal data. The ePrivacy Directive protects the confidentiality of communications and the integrity of terminal equipment. Blurring these legal logics would weaken protection at the point where tracking begins and creates confusion about which rules and authorities apply.

At the same time, we are deeply concerned with new reports that automated privacy signals are no longer on the table. The Council must reintroduce and strengthen this provision, avoiding watered-down language or delays in protections. Signals are the clearest example of genuine simplification in this file. They would allow people to express their choices through browsers, operating systems, apps, or other user-side tools, instead of being forced to navigate endless cookie banners. This would make rights easier to exercise and level the playing field for businesses that respect people's choices, rather than rewarding actors that rely on manipulative interfaces and non-compliant tracking.

The Council should therefore avoid the wrong shortcut: replacing signals with broad new exemptions from consent. Achieving fewer banners by removing the consent requirement and allowing tracking would be a false solution. It would increase risks for privacy, data protection, cybersecurity, and device integrity. Any consent-free access to terminal equipment must remain narrow, necessary, technically limited, and clearly safeguarded.

---

[1] Proposal for a Regulation amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024.

Where the Council keeps parts of the Commission proposal, it must add strong safeguards. Simplification cannot mean weaker transparency, weaker access rights, weaker protection for sensitive data, weaker complaint mechanisms, or weaker accountability for automated decision-making. The Council should also avoid using unresolved discussions on the Data Acquis to reopen progress made on GDPR and ePrivacy. If convergence is reached on the GDPR and ePrivacy parts, that compromise should be respected while discussions continue on the Data Acquis. Progress on one part of the file should not be used as an excuse to weaken another.

People and responsible organisations need rules that are clear, enforceable, and workable. But clarity cannot come from lowering safeguards, expanding tracking, or shifting the burden onto individuals to protect themselves. Legal certainty must mean rights that work in practice, obligations that can be enforced, and markets that reward responsible actors. A deregulatory race to the bottom will not make Europe more competitive. It will strengthen the actors that already dominate through scale, opacity, and data extraction, while leaving European businesses that try to comply on even less equal terms. Europe's digital sovereignty requires rules that make people's choices effective, enable enforcement, and allow rights-respecting businesses to compete fairly.

We urge Member States to adopt a Council position that protects the progress made so far: delete the most harmful proposals, keep ePrivacy and GDPR distinct, preserve automated privacy signals, prevent risky recitals from reviving deleted provisions, and reject any further deregulatory additions. A Data Omnibus that weakens rights will not deliver trust, legal certainty, or competitiveness. A rights-preserving mandate can.

Yours sincerely,

Attac Austria
ATTAC Spain
Bits of Freedom
Check My Ads
Corporate Europe Observatory (CEO)
Danes je nov dan
Defend Democracy
Ecologistas en Acción (Spain)
Electronic Frontier Foundation
Electronic Privacy Information Center (EPIC)
Elektronisk Forpost Norge | Electronic Frontier Norway
European Anti-Poverty Network
European Digital Rights (EDRi)
Homo Digitalis
IT-Pol
Panoptykon Foundation
People vs Big Tech
Politiscope
Privacy International
Stichting Data Bescherming Nederland
The Good Lobby