To Members of the European Parliament
and representatives of EU Member States,

One year later, simplification of our digital rights has gotten out of hand

We, the undersigned civil society organisations, consumer organisations, trade unions, academics, researchers, businesses and individuals, are deeply concerned about the direction of the so-called 'Digital Omnibus on Data' and the weakening of fundamental rights protections being pursued in the name of simplification and competitiveness.

A year ago today, the European Commission presented the Digital Omnibus Package as a simplification exercise. The proposed changes would drastically weaken protections for our fundamental rights to personal data protection and confidentiality of communications. By reopening long-established, future-proof concepts at the core of fundamental-rights law, they would also create more complexity and legal uncertainty.

The 'AI data grab' as an excuse to weaken the rules

The Digital Omnibus crosses the line from simplification to deregulation in several important areas, particularly when it comes to AI. We are repeatedly told that Europe needs more data, fewer constraints, and faster deployment if it wants to compete in the so-called AI race.

That race is not taking place on a blank page: while new competitors can and do emerge, key parts of the AI value chain remain highly concentrated. A small group of dominant technology companies have built their position through the accumulation and exploitation of vast amounts of data and other critical resources, including computing infrastructure, energy, natural resources, and capital. Their expansion has consequences for fundamental rights (within and beyond the EU), our environment, and ultimately who controls the technologies that increasingly mediate our societies.

The Digital Omnibus on Data would give AI development, training, and even operation a specific place under the GDPR's legitimate-interest framework. Creating a dedicated route for AI risks normalising large-scale reuse of personal data and shifting even more of the burden onto people to discover what is happening and object afterwards. The companies best placed to exploit such a framework are precisely those already holding the largest pools of data and the infrastructure to combine, infer and monetise them at enormous scale.

Our data should not become AI fuel by default, especially without us even knowing. Information collected for one purpose should not simply become available for another because a company has found a new commercial use for it. Nor should the law create incentives for companies to frame ever more processing as AI-related in order to benefit from more permissive rules.

More than just an AI problem

The AI data grab is only one part of a much wider reform. Other proposed changes could affect whether information, even the most intimate, about us receives protection in the first place; weaken safeguards for sensitive and biometric data; make automated decision-making easier to justify; make it harder to find out what organisations are doing with our data; and restrict rights that are often essential for uncovering profiling, discrimination or unlawful processing.

The proposals also reopen the rules protecting information stored on or accessed from our phones, computers and other connected devices. More permissive data access and reuse can also create security risks: the wider sensitive information circulates across complex commercial ecosystems, the more opportunities there are for misuse, compromise or access by hostile actors.

The few benefit; the many pay the price

All of us rely on these laws to set limits on how organisations can access the most intimate aspects of our lives. The Omnibus risks shifting the balance further away from people, with some groups carrying much greater risks:

- Workers and trade unions: weaker safeguards around automated decisions, profiling, and access rights can make recruitment, workplace surveillance, performance management, or dismissal harder to understand and challenge;

- Patients and people relying on public services or social protection: broader possibilities to reuse data and weaker rights to information, access and challenge can affect healthcare, benefits, housing, education and other essentials;

- Racialised people, migrants and LGBTQIA+ people: profiling and automated systems can affect access to services, mobility, opportunities and equal treatment, while strong access and transparency rights are often essential for uncovering discrimination and harmful inferences;

- Journalists, human rights defenders and their sources: confidentiality of communications and device integrity are basic conditions for doing their work safely and for an enabling civic space;

- Consumers, in particular children and young people, including students: weaker protections risk shifting even more responsibility onto them to resist commercial tracking and data extraction, while EU institutions simultaneously promise to make the digital environment safer for them;

- Ethical businesses, universities and researchers: companies investing in privacy-protective and rights-respecting products should not be disadvantaged against competitors with greater capacity to extract data, absorb legal risk or push regulatory boundaries. Reopening core concepts can also increase uncertainty and compliance costs across supply chains, while commercial actors should not be able to benefit too easily from exemptions designed to protect genuine scientific inquiry.

Rights deserve evidence

These reforms concern the GDPR and ePrivacy rules, which implement rights protected by Articles 7 and 8 of the Charter of Fundamental Rights. Any limitation of those rights must be necessary and proportionate. Yet changes of this scale have been proposed without the kind of impact and proportionality assessment, public scrutiny and consultation that substantive interference with fundamental rights requires.

This is part of a wider problem. Far-reaching changes across different areas of EU law are increasingly being bundled into fast-moving Omnibus packages designed around speed and burden reduction. Rules that took years of democratic negotiation should not be substantially rewritten without evidence that doing so will actually deliver the innovation or competitiveness being promised.

There is still time to change course: what we are asking EU lawmakers to do

One year on, EU lawmakers still have a chance to change course. We ask the European Parliament and Member States to reject the provisions of the Digital Omnibus that weaken substantive rights and safeguards. Where genuine problems in the GDPR, ePrivacy or other legislation merit reform, they should be addressed openly and meaningfully through proper legislative initiatives, with evidence, impact assessments, participatory consultations with civil society and full democratic scrutiny, for instance as part of the Digital Fitness Check. In particular, EU lawmakers should:

- reject a redefinition of the concept of personal data, either via Article 4 GDPR or indirectly via other provisions blurring the distinction between pseudonymised and anonymised data;
- reject privileged routes for large-scale reuse of personal data for AI and, if controllers want to use legitimate interest as their legal basis for AI development, preserve an effective three-step test with meaningful purpose limitation, data minimisation, concrete safeguards, as well as genuine choice for data subjects including an unconditional right to object;
- maintain strong protection for sensitive and biometric data;
- keep meaningful safeguards around automated decisions, including genuine human intervention and the ability to understand and challenge decisions;
- protect effective rights to information and access to personal data;
- ensure that the research exception remains limited to scientific purposes aimed at serving the public good with appropriate institutional safeguards;
- preserve strong, preventive protection against access to information on people's devices, while making automated privacy signals binding so that people can express their choices once and have them respected.

That is the choice in front of EU lawmakers: simplify the rules where they genuinely need simplifying, do not simplify away our rights.

Signed,

Civil society, consumer and trade union organisations

- Access Now
- AK EUROPA
- AlgorithmWatch
- Alternatif Bilişim
- Asociația pentru Tehnologie și Internet (ApTI)
- Balanced Economy Project
- Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V
- BEUC - The European Consumer Organisation
- Bits of Freedom
- Centar za građanske inicijative Poreč
- Centre for Democracy and Law Miko Tripalo
- Centre for Democracy and Technology Europe (CDT Europe)
- Check My Ads
- Child Rights International Network (CRIN)
- Civil Liberties Union for Europe (Liberties)
- Corporate Europe Observatory (CEO)
- Danes je nov dan, Inštitut za druga vprašanja
- Data for Good
- Data Justice Europe
- DECO - Associação Portuguesa para a Defesa do Consumidor
- Defend Democracy
- Die Bürokratiemonster
- Digitalcourage
- Digitale Gesellschaft (CH)
- Digitale Gesellschaft (Germany)
- European Coalition for Corporate Justice
- European Digital Rights (EDRi)
- European Disability Forum (EDF)
- Electronic Frontier Norway (EFN)
- Enforce
- Eurocadres
- European Public Service Union (EPSU)
- Federación de Consumidores y Usuarios CECU
- Forbrugerrådet Tænk
- Gong
- Hermes Center Hacking for Human Rights
- Homo Digitalis
- Human Rights House Zagreb
- Human Rights in Finance (EU)
- Irish Council for Civil Liberties (ICCL)
- Initiative für Netzfreiheit

- IT-Pol Denmark
- Ius Omnibus
- KEPKA
- Kettensäge stoppen!
- La Quadrature du Net
- Lafede - justícia global
- LDH (Ligue des droits de l'Homme/droits humains)
- LobbyControl
- Norwegian Consumer Council (Forbrukerrådet)
- noyb
- Oxfam
- Panoptykon Foundation (PL)
- People vs Big Tech
- Platform for the International Cooperation on Undocumented Migrants (PICUM)
- Politiscope
- Privacy First
- Privacy International
- Ranking Digital Rights (RDR)
- Statewatch
- The Business and Human Rights Centre
- The Firewall
- The Good Lobby
- Tournesol.org
- Verbraucherzentrale Bundesverband (vzbv) - Federation of German Consumer Organisations
- VSCyberH

Academics and researchers

- Harshvardhan Pandit, AI Accountability Lab, Trinity College Dublin
- Cristiana Sappa, professor of business law, IESEG School of Management
- Ass.-Prof. Dr. Soheil Human, Director of the Sustainable Computing Lab, Vienna University of Economics and Business
- Sophie Stalla-Bourdillon, Co-Director of the Brussels Privacy Hub, Science, Technology and Society (LSTS) Research Group, Vrije Universiteit Brussel (VUB)
- Associate Professor Derya Ozkul, University of Warwick
- Dr Plixavra Vogiatzoglou, postdoctoral researcher at the Amsterdam Law School
- Dr. Ariadna Matamoros-Fernandez, Associate Professor of Information and Communication Studies at UCD
- Dr. Felix Bieker, LL.M., FIZ Karlsruhe – Leibniz Institute for Information Infrastructure
- Dr. Guido Gorgoni, Professor of Digital Citizenship and European Citizenship, University of Padova, Italy
- Dr. Irene Kamara, associate professor
- Dr. Lorenzo Dalla Corte, assistant professor in data protection and cybersecurity law, Tilburg University
- Dr. Nicole Gross, Associate Professor of Business & Society at the National College of Ireland
- Emeritus professor of international law

- judith membrives i llorens, Assistant professor at UOC
- Kristina Irion, Associate Professor, Institute for Information Law, University of Amsterdam
- Mariavittoria Catanzariti
- Prof. Dr. Gloria González Fuster, Director of the Law, Science, Technology and Society (LSTS) Research Group, Vrije Universiteit Brussel (VUB)
- Prof. Maurizio Borghi, University of Turin, co-director NEXA Center for Internet & Society
- Sara Garsia, Doctoral Researcher at the Centre of IT and IP Law of KU Leuven
- Marco Giraudo, Università di Torino

Businesses and companies

- Cryptee
- Element
- fix the status quo
- Freedom Internet BV
- Hostsharing eG
- Legally Mel srl
- lolongo
- New School of the Anthropocene
- Tuta

Individuals

- Jutta de Mendelssohn-Schwarz, Artist
- Conor Hogan, Data protection and cybersecurity professional
- Dr Aida Ponce Del Castillo
- Wolfie Christl, senior researcher at Cracked Labs (Vienna) and The Citizen Lab (University of Toronto)
- Xavier Brandao, independent expert