Dear Members of the European Parliament,

The undersigned organisations urge the European Parliament to ensure a high level of protection of privacy and confidentiality in the upcoming ePrivacy Regulation and to address the weakness in the current Council position during trilogue negotiations.[1]

Four years ago, the European Commission proposed the ePrivacy Regulation to complete the modernisation of the EU data protection framework begun by the GDPR. **To address the concerns related to the use of cookies and other tracking technologies**, the European Parliament adopted several provisions[2] that:

- **Protect Internet users from tracking and monitoring, whether by cookies or other technological means.** The collection of data from, or storage of data on, a user's device is allowed only with the consent of the user unless technically required for the service (Article 8);

- **Prohibited tracking or cookie walls**, which seek to coerce users into 'consenting' to the processing or storage of additional data in exchange for access (Article 8)

---

1 2021 Council of the European Union mandate for negotiations with EP, available at: https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf

2 2017 Draft European Parliament Resolution on the Regulation on Privacy and Electronic Communications, available at: https://www.europarl.europa.eu/doceo/document/A-8-2017-0324_EN.html

- **Lightened the burden of privacy controls on Internet users**, by allowing them to automate consent choices and use legally binding signals sent by network-connected software or hardware[3] to communicate them to websites (Articles 9 and 10). Article 19 set out a process for the specification of such signals by the European Data Protection Board.

These protections were removed or weakened by the Council in its negotiation mandate.

The Council's Article 8(1) letters a, c and d create ambiguity about the data that are "technically necessary" for a service and open the door to the tracking of users. Furthermore, the prohibition against "tracking walls" has been moved to a Recital and qualified with unclear caveats.

Council also deleted Articles 9 and 10, backing away from technical solutions to the constant requests to agree to further data collection. As a consequence, users will have to face the continued nuisance of consent banners which try to manipulate them with 'dark patterns'. These requests could instead be dealt with by legally binding signals configured by the user, but this solution has now been abandoned to wishful thinking and relegated to a Recital. As regards privacy by design and default, **most browsers have shifted to protecting their users, an evolution which the Regulation has not taken account of and should expand on.**

Since the Parliament agreed its position in October 2017, public trust in data collection has been damaged by the Cambridge Analytica scandal. The ePrivacy regulation must send a clear message that the future belongs to business models which unify fundamental rights and innovation, rather than those who operate a personal data dragnet.

The Council position, instead, legitimises abuses and breaches of data protection law and fails to address the trust deficit. In 2016, a Eurobarometer survey found that "more than seven in ten Internet and online platform users agree they are concerned about the data collected about them on the Internet".[4] In 2020, studies have found that a third of consumers acted upon these concerns, and terminated their relationship with at least one business because of data privacy concerns.[5] The same study found that another 87% of respondents was worried about their data not being protected by the tools they need to use for remote working because of the COVID-19 pandemic.

3 Including browsers, operating systems, and IOT devices.

4 2016 Special Eurobarometer 447: online platforms, available at: https://data.europa.eu/euodp/en/data/dataset/S2126_85_1_447_ENG

5 Cisco 2020 Consumer Privacy Survey, available at: https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cybersecurity-series-2020-cps.pdf

We urge the European Parliament to reassert their position and ensure that the ePrivacy Regulation delivers on its objectives. Personal data in the field of electronic communications are extremely sensitive, as they reveal intimate aspects of the private life of individuals, particularly during the COVID-19 pandemic when everyday activities and exchanges are now largely happening online. Therefore, **the protection afforded by the GDPR should be complemented by closing loopholes and grey areas that have been widely abused by the tracking industry, as well as by providing additional, stronger guarantees to personal data processing in that field.**

We call on the European Parliament to take full account of the opinions of the European Data Protection Board and the European Data Protection Supervisor, and to reject any proposal or compromise that would lower the level of, protection provided by the GDPR and the current ePrivacy Directive.

Yours sincerely,

- Access Now, International
- Amnesty International
- BEUC, The European Consumer Organisation
- Bits of Freedom, The Netherlands
- Centre for Peace Studies, Croatia
- Civil Liberties Union for Europe (Liberties), International
- Civil Rights Defenders, Sweden
- Coalition for Civil Liberties and Rights, Italy
- Communia, International
- Deutsche Vereinigung für Datenschutz e.V. (DVD), Germany
- Digitalcourage, Germany
- Electronic Frontier Foundation, International
- Free Knowledge Advocacy Group EU, International
- Homo Digitalis, Greece
- Human Rights Monitoring Institute, Lithuania
- Hungarian Civil Liberties Union, Hungary
- Institute of Information Cyprus, Cyprus
- IT-Pol Denmark, Denmark
- Liga lidských práv | League of Human Rights, Czech Republic
- Ligue des Droits Humains, Belgium
- Netzwerk Datenschutzexpertise, Germany
- Open Rights Group, United Kingdom
- Panoptykon Foundation, Poland
- Platform Bescherming Burgerrechten, The Netherlands
- Privacy First, The Netherlands
- Privacy International, International
- Ranking Digital Rights, USA
- The Irish Council for Civil Liberties, Ireland
- The Privacy Collective, International
- Xnet, Spain