Dear Members of Parliament, Dear Co-Rapporteurs MEP Kaljurand and MEP Salla,
Dear Permanent Representatives, Dear Ambassador O'Donoghue,
Dear Executive Vice President Virkkunen and Commissioner McGrath,

Subject: Joint call to replace cookie banners with automated signals (Article 88b proposal for a Digital Omnibus COM(2025) 837 final)

We, the undersigned leading civil society organisations defending digital rights of people in the EU, and representing the interest of consumers, academics and businesses across Europe, have gathered in a coalition named "Kill the cookie banner" (killthecookiebanner.eu). Our aim is to ensure that EU law finally puts an end to annoying and misleading cookie banners. This is necessary to diminish illegal commercial surveillance, to reduce unlawful tracking and interference with people's devices and communications, while simplifying and tangibly improving the lives of all Europeans, consumers and businesses alike, and opening the door to meaningful innovation.

The European Commission took the long overdue initiative to kill cookie banners by proposing to introduce an obligation to respect automated signals that communicate users' privacy choices. The proposal is included in the pending Digital Omnibus (Article 88b) and is the only "simplification" measure that would actually benefit people in this package of mainly business-oriented and protection-reducing measures.

Automated signals would allow users to automatically communicate their preferences concerning the access to and use of their devices, tracking, and the processing of personal data. At the same time, they would simplify the exercise of their privacy and data protection rights, enabling them to make their privacy choices upfront. These choices are then automatically communicated to websites, apps and other services the user engages with. This way, consumers do not have to interact with hundreds of different and often misleading cookie banners anymore.

We are united in strong support for the introduction of automated signals as the solution to overcome the perceived nuisance of "consent banners".

Why Europe needs to do better for European consumers and businesses regarding privacy choices

The EU needs to deliver real simplification that people (and voters) can see in their everyday life, rather than merely reducing the obligations for businesses. Putting an end to consent banners as proposed by the European Commission would be highly popular with European voters. At a time where the European Union is keen to deliver on its simplification agenda, which often unilaterally benefits businesses, the introduction of an automated signal is a win-win for all: For consumers, but also for the majority of businesses who will profit from less interruptions in their core services by not having to show cookie banners on their websites, apps, and other online services anymore.

Automated opt-out signals, such as Global Privacy Control (GPC), are already being standardised and are legally binding in several US states. At the same time, more comprehensive frameworks,

such as Advanced Data Protection Control (ADPC[1]), are being developed, which not only enable users to opt-out, but also opt-in to specific purposes and controllers, potentially getting rid of most cookie banners. The proposed Article 88b also mandates developing a European standard, which would build on the existing signals to allow for a more efficient communication of choices while upholding compliance with the standards for consent under the GDPR. This would not change the rights of people or the general duties of businesses at all. Instead, a legally mandated, European standard, technically developed within the EU standardisation body with an active participation of civil society organisations, will remove unnecessary burden from people, maintain the highest level of protections for people's rights, and facilitate a legitimate and thriving online economy.

In the debate over the past few months, we witnessed widespread confusion due to the lack of technical knowledge about existing solutions, as well as inaccurate assumptions about the application and impact of the proposed Article 88b. Some stakeholders have deliberately painted Article 88b as being a "kill switch". This reading is incorrect and at odds with what the Commission proposed. Instead, the proposed solution is a more nuanced approach allowing for consent or the refusal of consent in advance, thereby keeping users safe from undue influence through deceptive design in cookie banners. It would reduce repetitive consent requests while allowing people to exercise their choices more effectively.

What is needed for Article 88b to become a major success for the EU

All the ingredients are on the table for Article 88b to become a success. Automated signals are nothing new. Technical concepts for privacy signals were already developed in the 2000s. So far, however, the legal framework and a standard have been missing in the EU.

But this would be provided by an improved Article 88b: It should mandate the use of signals for the expression of consent, for the withdrawal and refusal of consent, as well as for the objection to the processing of personal data. Of course, consent through such a signal should meet all the requirements of the GDPR. Importantly, the law should prevent dominant companies from being in a position to impose their preferred options on users by managing their choices.

Please find in the annex to this letter a set of more detailed recommendations for the elements Article 88b should comprise to ensure that automated signals are effective and that the European Commission can give a clear, democratically legitimised and robust mandate to the European standardisation organisations.

Call to improve and adopt Article 88b

Europeans have been waiting far too long for a simple way to exercise meaningful choices about tracking, access to their devices and the use of their personal data.

We therefore call on the Irish presidency, ambassador Aingeal O'Donoghue, to re-insert Article 88b into their next compromise text and recommence the discussion with Member States.

We call on Member States who have expressed doubts about the introduction of automated signals to reconsider their position and to support Article 88b in an improved version.

1 ADPC developed by the Vienna University of Economics and some civil society groups including noyb

We call on MEPs of all political groups and in particular on the co-rapporteurs, MEP Kaljurand and MEP Salla, to do their utmost to broker an effective solution based on the many constructive amendments that have been tabled in the respective Parliamentary Committees on Article 88b, effectively killing cookie banners. The European Parliament as the institution who represents people must show the way to positive innovation and simplification in the interest of all.

We call on the European Commission, represented by Commissioner McGrath and EVP Virkkunen, to strongly defend and advocate for this welcome initiative, which is the only genuine simplification measure that benefits users and to make it a political priority of the Digital Omnibus.

People would find it hard to understand if the responsible decision makers were to maintain cookie banners and to reject the Commission's proposal for Article 88b. Failing to establish a workable and binding system for automated signals would leave people stuck with the very consent-banner model that so many across the EU complain about and agree needs to change. Europeans would applaud "Brussels" for finally taking measures to make their lives easier and to protect their privacy choices.

We count on you, and we are, of course, at your disposal should you require any further information.

Sincerely,

The "Kill the cookie banner" campaign members

Annex: 1

ANNEX to letter: **Joint call to replace cookie banners with automated signals**

Article 88b should oblige companies to accept automated communication of privacy preferences by users and should include the following elements:

- The consent given via such a signal should meet all the requirements of Article 4(11) GDPR. In particular, signals must allow for the expression of choices per controller and per purpose, which allows to send different signals to a trusted local newspaper than to an international data-hungry platform.
- Providers and other actors accessing information in terminal equipment should be required to respect legally valid automated signals. If a signal expresses refusal, withdrawal or objection, it should prevent the corresponding access or processing and should take precedence over subsequent consent requests concerning the same processing, unless the user actively changes their choice.
- Dominant companies (e.g. gatekeepers like Google, in relation to browsers) should not be able to design or manage automated signals for users in a way that further entrenches their market power. Dominant browsers and mobile operating systems should be required to facilitate that users can send their preference signal (like under the respective California law[2]).
- The legal meaning, scope and effect of automated signals should be sufficiently detailed and determined by Union law to give a clear mandate for the European Standardisation Bodies. Technical standards should be limited to ensuring interoperability and technical implementation and must not redefine or weaken users' rights. The standardisation process should be inclusive, timely and enable effective supervision and enforcement. Relevant civil society organisations must be invited to the standardisation process.
- Signals expressing refusal, withdrawal or objection should remain effective over time until changed by the user. Providers should not circumvent them through repeated consent requests, interface design, changes in terminology or other technical means. Users should not face degraded access or functionality merely because they have communicated refusal, withdrawal or objection through an automated signal.
- Browsers, operating systems, applications and independent user agents must be able to transmit signals without gatekeeper interference and/or additional tracking.

2 California "Opt Me Out" Act, AB 566