

ACCESS TO AND STORAGE OF DATA ON TERMINAL EQUIPMENT

Context

The narrow exemptions of Article 5 of the ePrivacy Directive (2002/58/EC) have led to absolutist interpretations that effectively reduce the regime to a “consent-first” model, making even low-risk or anonymous data uses, such as basic analytics, unnecessarily complex.

It creates significant difficulties for vehicle manufacturers seeking to transfer data out of vehicles; any time the onboard telematics unit or sensors send data externally, it may qualify as “accessing/storing information” under Article 5(3). This challenge is compounded by the fact that a vehicle is rarely used by a single individual; it may be driven by the owner, a family member, an employee, or a short-term renter, with passengers also potentially implicated.

ACEA supports the European Commission’s objective to update the consent mechanism provided under Article 5(3) of the ePrivacy Directive, but the consent requirement under the Commission’s proposal does not resolve the situation.

The exceptions in paragraph 3 are too narrow to help solve the issues raised by the consent-first mechanism currently applicable under the ePrivacy Directive and effectively reprised in this proposal. Furthermore, it requires the existence of a service requested specifically by a natural person, as a condition for the lawfulness of data processing, thereby creating additional restrictions compared to the ePrivacy Directive, which refers to the notion of “subscriber”, which can be either a natural or a legal person (Article 5(3)).

Recommendation

1. **The proposal for an Article 88a GDPR should be deleted** to avoid created overlapping yet incompatible regimes which provide little assistance to data controllers and create legal uncertainty.
2. **Article 5 of the ePrivacy Directive should be amended to include clear and necessary exception to the consent rule** where the purpose of the storing of or access to information in terminal equipment has the potential to create societal benefits, especially regarding people’s health, safety or security, or where they can benefit the environment.

Rationale

This targeted amendment is a pragmatic and proportionate solution which preserves the core of the consent rule, but introduces narrowly framed exceptions defined by law, for purposes which are strictly necessary and demonstrably beneficial

This solution corrects of a system that currently produces legal uncertainty, consent fatigue and poorly informed choices, and a structural disincentive for European companies to deploy socially valuable, privacy-respecting services.

This solution would improve protection for individuals because processing would occur only where objectively justified and regulated, rather than hidden behind formalistic consent flows. It would also provide legal certainty for controllers wishing to deploy privacy-respecting technologies for socially valuable services, who currently face legal risk or are forced into ineffective consent mechanisms that neither serve users nor innovation.

Proposal for amendments

Proposal for a regulation	
Article 3, para. (15)	
Text proposed by the Commission	Amendment
15. After Article 88, the following articles are added: ‘Article 88a Processing of personal data in the terminal equipment of natural persons (1) Storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person is only allowed when that person has given his or her consent, in accordance with this Regulation. (2) Paragraph 1 does not preclude storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person, based on Union or Member State law within the meaning of, and subject to the conditions of Article 6, to safeguard the objectives referred to in Article 23(1). (3) Storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person without consent, and subsequent processing, shall be lawful to the extent it is necessary for any of the following: (a) carrying out the transmission of an electronic communication over an electronic communication network; (b) providing a service explicitly requested by the data subject; (c) creating aggregated information about the usage of an online service to measure the audience of such a service, where it is carried out by the controller of that online service solely for its own use;	Deleted

<i>(d) maintaining or restoring the security of a service provided by the controller and requested by the data subject or the terminal equipment used for the provision of such service.</i> <i>(4) Where storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person is based on consent, the following shall apply:</i> <i>(a) the data subject shall be able to refuse requests for consent in an easy and intelligible manner with a single-click button or equivalent means;</i> <i>(b) if the data subject gives consent, the controller shall not make a new request for consent for the same purpose for the period during which the controller can lawfully rely on the consent of the data subject;</i> <i>(c) if the data subject declines a request for consent, the controller shall not make a new request for consent for the same purpose for a period of at least six months.</i> <i>This paragraph also applies to the subsequent processing of personal data based on consent.</i> <i>(5) This Article shall apply from [OP: please insert the date = 6 months following the date of entry into force of this Regulation]</i>	
<u>Justification:</u> The consent requirement under Article 88a reprises the consent-first mechanism currently applicable under the ePrivacy Directive, and the exceptions to this requirement provided under paragraph 3 are too narrow to help solve the issues raised by the mechanism. The Commission’s proposal appears too focused on cookies and does not reflect the reality of the wider Internet of Things (IoT), including connected motor vehicles.	

Text proposed by the Commission	Amendment
NEW	Article 4(a) Amendment to Directive 2002/58/EC Directive 2002/58/EC is amended as follows: 1. In Article 5, the following paragraphs are added: ‘4. Paragraph 3 shall not apply where the storing of information, or the gaining of access to information already stored in the terminal equipment of a user or subscriber, is strictly necessary for processing operations that demonstrably create, or have the potential to create, significant societal benefits, in accordance with paragraph 5.’ 5. Processing under paragraph 4 shall only apply where the storing of or access to information in terminal equipment is strictly necessary to further a purpose with the potential to create societal benefit. For the purposes of this paragraph, “societal benefit” includes, inter alia: (a) road safety, transport safety, and accident prevention, including the operation, maintenance, and improvement of connected vehicles and mobility systems; (b) public health, epidemiological monitoring, and health-related research; (c) cybersecurity, detection and remediation of vulnerabilities, and resilience of critical infrastructure; (d) environmental protection, climate-related monitoring, and energy efficiency; (e) scientific research and innovation activities with broad societal relevance; (f) other purposes listed in implementing acts adopted under Article 5(3b).’ ‘6. The Commission is empowered to adopt implementing acts establishing and regularly updating a Unionwide list of processing operations that qualify as societal benefit purposes under paragraph 5. 7. Paragraph 3 shall not prevent the storage of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user, insofar as

	<i>such storage or access is strictly necessary for the purpose of complying with an obligation laid down in Union or Member State law</i> 2. After article 5, the following article is added: Article 5a Exercised of the delegation 1. The implementing acts referred to in article 5 shall specify: (a) <i>categories of processing operations considered to generate significant societal benefits;</i> (b) <i>minimum safeguards and technical standards required for such operations;</i> (c) <i>conditions for inclusion or removal of processing operations from the list.</i> 2. In preparing these implementing acts, the Commission shall take into account: (a) <i>the expected societal benefits, including in the fields of safety, public health, environment, scientific research, innovation, and cybersecurity;</i> (b) <i>risks to fundamental rights and freedoms;</i> (c) <i>the availability of less intrusive means;</i> (d) <i>evidence from scientific, industrial, and regulatory stakeholders.</i> 3. The Commission shall consult the European Data Protection Board and the European Union Agency for Cybersecurity (ENISA), which shall issue an opinion within eight weeks of receiving a draft implementing act. 4. The implementing acts referred to in this Article shall be adopted in accordance with the examination procedure laid down in Article 14a(2).' 3. Article 14a is replaced by the following: 'Article 14a Committee procedure 1. The Commission shall be assisted by a committee within the meaning of Regulation (EU) No 182/2011.
--	---

	<i>2. Where reference is made to this paragraph, the examination procedure under Article 5 of Regulation (EU) No 182/2011 shall apply.</i>
<u>Justification:</u> Strict reliance on consent for any access to or storage of information on terminal equipment has led to legal uncertainty, consent fatigue and poorly informed choices, and a structural disincentive for European companies to deploy socially valuable, privacy-respecting services. Introducing a carefully framed, purpose-based exception system in Article 5(3) of the ePrivacy Directive would improve protection for individuals because processing would occur only where objectively justified and regulated, rather than hidden behind formalistic consent flows. It would also provide legal certainty for controllers wishing to deploy privacy-respecting technologies for socially valuable services, who currently face legal risk or are forced into ineffective consent mechanisms that neither serve users nor innovation.	