

LAW AND DIGITAL TECHNOLOGIES ELECTRONIC COMMUNICATIONS

ePrivacy

Prof. G-J. (Gerrit-Jan) Zwenne
February 5th, 2025



HOME > EU DATA PROTECTION > COUNCIL OF THE EU RELEASED A (NEW) DRAFT OF THE EPRIVACY REGULATION

Council of the EU Released a (New) Draft of the ePrivacy Regulation

By Dan Cooper and Anna Oberschelp de Meneses on January 6, 2021

POSTED IN DATA PRIVACY, EU DATA PROTECTION, EUROPEAN UNION, GDPR

On January 5, 2021, the Council of the European Union released a new **draft version** of the ePrivacy Regulation, which is meant to replace the ePrivacy Directive. The European Commission approved a first draft of the ePrivacy Regulation in January 2017. The draft regulation has since then been under discussion in the Council.

On January 1, 2021, Portugal took over the presidency of the Council for six months. Ahead of the next meeting of the Council's working party responsible for the draft ePrivacy Regulation, the **Portuguese Presidency** issued a revised version of the draft regulation. This is the **14th draft version** of the ePrivacy Regulation (including the European Commission's first draft).

Once approved, the ePrivacy Regulation will set out requirements and limitations for publicly available electronic communications service providers ("service providers") processing data of, or accessing devices belonging to, natural and legal persons "who are in the [European] Union" ("end-user"). The regulation aims to safeguard the privacy of the end-users, the confidentiality of their communications, and the integrity of their devices. These requirements and limitations will apply uniformly in all EU Member States. However, EU Member States have the power to restrict the scope of these requirements and limitations where this is a "necessary, appropriate and proportionate measure in a democratic society to safeguard one or more of the general public interests."





24/01/2025 A proposal for a regulation on the respect for private life and the protection of personal data in electronic communications (proposal for e-Privacy Regulation) has been published on **10 January 2017**.

In the European Parliament (EP), the file was assigned to the Civil Liberties Committee (LIBE) and the initial rapporteur, MEP Marju Lauristin (Estonia, S&D), presented the report in **June 2017**, aimed at strengthening the confidentiality of communications including in machine-to-machine communications. The EP confirmed the committee's negotiating mandate in **October 2017** and since then, Birgit Sippel (Germany, S&D) took over as responsible MEP. She has been re-appointed as rapporteur on 30 September 2024.

The European Data Protection Authorities (DPAs), assembled in the EDPB (European Data Protection Board), adopted in **March 2018** an opinion on the interplay between the e-Privacy Directive and GDPR (in particular on the competences of DPAs). They also called not to lower the level of protection offered by the current e-Privacy Directive.

In the Council, the discussions were stalled for approx. **four years**.

In July 2020, the German Presidency published its first discussion paper. National delegations recently rejected a revised version of the paper and on **23 November 2020** the German Presidency presented its progress report, stating it

would 'closely [work] with the forthcoming Portuguese Presidency to facilitate further discussions and to ensure smooth progress on the file'. The initiative was **given utmost priority** in the Joint Declaration of the European Parliament, the Council and the European Commission from **17 December 2020**. On

10 February 2021, the Member States agreed on a mandate for negotiations with the European Parliament and trilogues began on **20 May 2021**.

On **28 March 2022**, the former French Presidency released its latest four column table in preparation of the trilogues. Some progress was made at a technical level under the Czech Council Presidency (**1 July to 31 December 2022**), but the file stalled again under the Swedish Council Presidency (**1 January to 30 June 2023**). Work on the file is planned to resume during the current parliamentary term



Directive (EU) 2018/1972 of 11 December 2018 establishing the European Electronic Communications Code (Telecoms Code)

Art. 2(4)

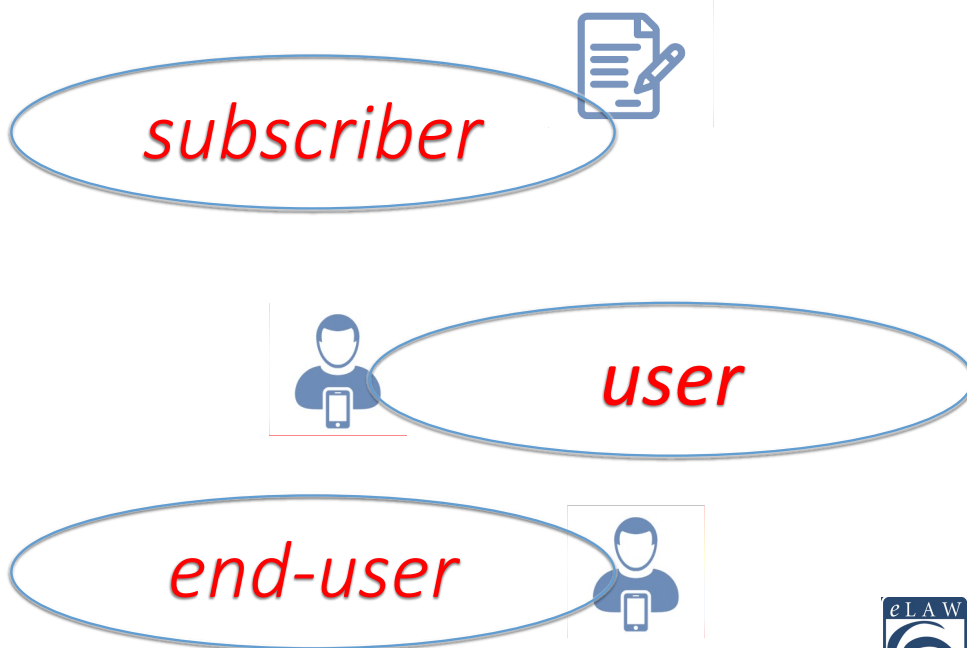
‘electronic communications service’ means a service normally provided for remuneration via electronic communications networks, which encompasses, with the exception of services providing, or exercising editorial control over, content transmitted using electronic communications networks and services, the following types of services

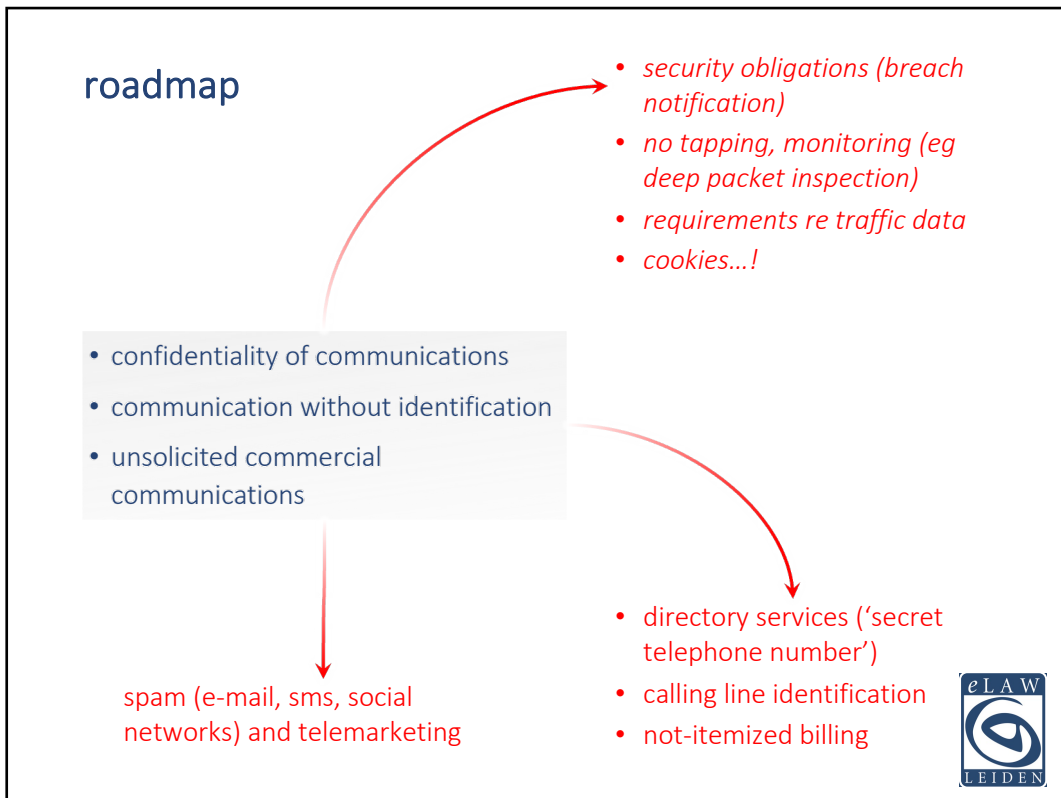
- (a) ‘internet access service’ as defined in point (2) of the second paragraph of Article 2 of Regulation (EU) 2015/2120;
- (b) **interpersonal communications service**
- (c) services consisting wholly or mainly in the conveyance of signals such as transmission services used for the provision of machine-to-machine services and for broadcasting

Over The Top (“OTT”) Services e.g. Whatsap, Signal, Telegram etc. Facebook? X

Art. 2(5)

a service normally provided for remuneration that enables direct interpersonal and interactive exchange of information via electronic communications networks between a finite number of persons, whereby the persons initiating or participating in the communication determine its recipient(s) and does not include services which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service






CONFIDENTIAL

CONFIDENTIAL

CONFIDENTIAL

confidentiality of communications


eLAW
LEIDEN




security obligation

appropriate technical and organisational measures to safeguard security of the [electronic communication] services, if necessary in conjunction with the provider of the public communications network with respect to network security

having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.






breach notification

- notify the personal data breach to the competent national authority
- also notify the subscriber or individual, if likely to adversely affect the personal data or privacy of a subscriber or individual, of the breach without undue delay

*24 hours? 72 hours?
what's the startingpoint?*



breach notification to DPA

In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority [...], unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons

notification to data subject

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.



Meldloket datalekken Autoriteit Persoonsgegevens

Een nieuwe melding indienen

Gegevens over het datalek

authenticatie... ?

Art. 6 EPR
Art. 5(1) ePD

“electronic communications metadata”

confidentiality of communications and traffic data


no listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned

deep packet inspection (“dpi”)

↑

net neutrality debat...

spam filter..?




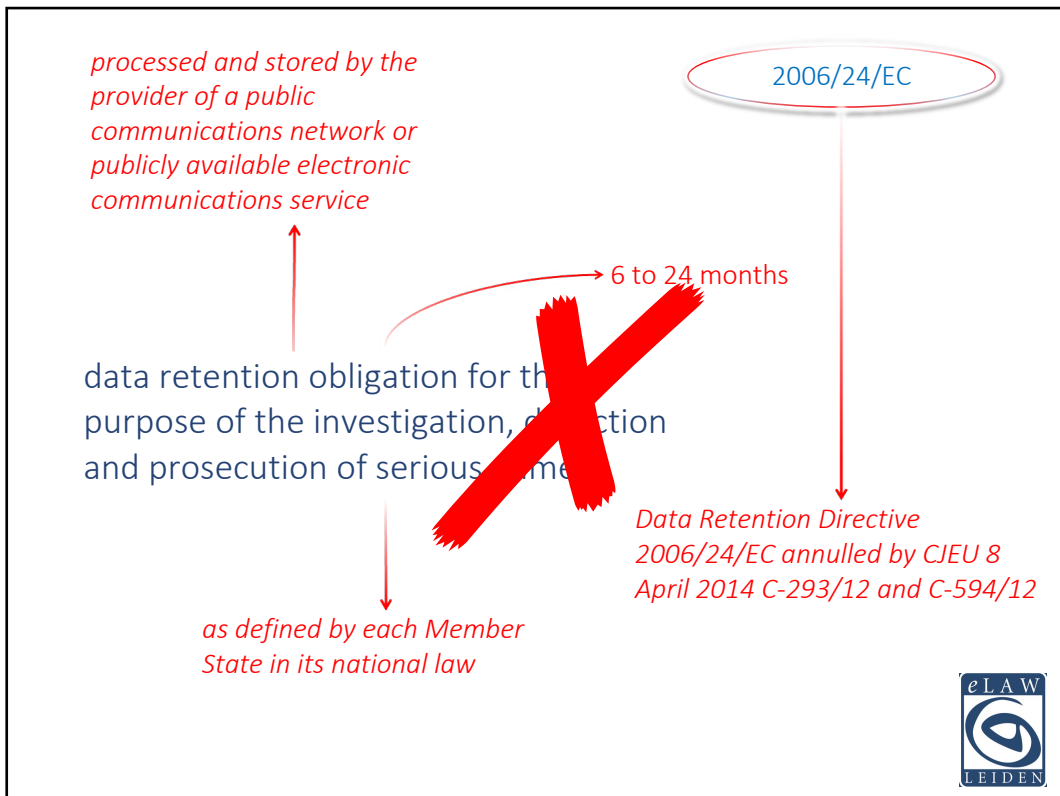
Art. 6 ePD

traffic data relating to subscribers and users must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication

↘

with user or subscriber data may be used for the purpose of marketing electronic communications services or for the provision of value added services.





Autorité de protection des données
Gegevensbeschermingsautoriteit

THEMES ▾ PRIVACY ▾ ACTIONS ▾ PUBLICATIONS ▾ THE AUTHORITY ▾ PRESS ▾

02 FEB 2022

The BE DPA to restore order to the online advertising industry: IAB Europe held responsible for a mechanism that infringes the GDPR

The Belgian DPA has found that the Transparency and Consent Framework (TCF), developed by IAB Europe, fails to comply with a number of provisions of the GDPR. The TCF is a widespread mechanism that facilitates the management of users' preferences for online personalised advertising, and that plays a pivotal role in the so called Real Time Bidding (RTB). The BE DPA imposed a €250.000 fine to the company, and gives IAB Europe two months to present an action plan to bring its activities into compliance.



CJEU 7 Mach 2024, C-604/22
ECLI:EU:C:2024:214
(IAB Europe)

Main findings : the TCF implies the processing of personal data

Contrary to IAB Europe's claims, the Litigation Chamber of the BE DPA found that IAB Europe is acting as a data controller with respect to the registration of individual users' consent signal, objections and preferences by means of a unique Transparency and Consent (TC) String, which is linked to an identifiable user. This means that IAB Europe can be held responsible for possible violations of the GDPR.

The BE DPA identified a series of GDPR infringements by IAB Europe :

- **Lawfulness** : IAB Europe failed to establish a legal basis for the processing of the TC String, and the legal grounds offered by the TCF for the subsequent processing by adtech vendors are inadequate;
- **Transparency and information of the users** : the information provided to users through the CMP interface is too generic and vague to allow users to understand the nature and scope of the processing, especially given the complexity of the TCF. Therefore it is difficult for users to maintain control over their personal data;
- **Accountability, security and data protection by design/by default** : In the absence of organisational and technical measures in accordance with the principle of data protection by design and by default, including to ensure the effective exercise of data subject rights as well as to monitor the validity and integrity of the users' choices, the conformity of the TCF with the GDPR is not adequately warranted nor demonstrated;
- **Other obligations pertaining to a controller processing personal data on a large-scale**: IAB Europe has failed to keep a register of processing activities, to appoint a DPO and to conduct a "DPIA" (data protection impact assessment).



Art. 8 ePR

Art. 5(3) ePD

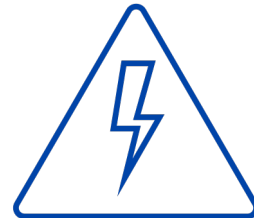
cookies, pixels etc..

the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information

but functional or technical cookies are allowed nevertheless



where technically possible and feasible [...] consent may be expressed by using the appropriate technical settings of a software application enabling access to the internet.



Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment



CNIL
To protect personal data, support innovation, promote individual liberties

MY COMPLIANCE TOOLS | DATA PROTECTION | THE CNIL | Q | T

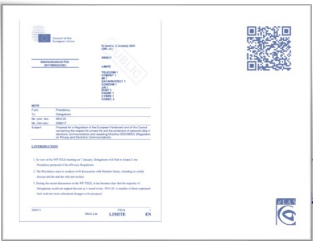
Home > Cookies and other tracking devices: the Council of State issues its decision on the CNIL guidelines

Cookies and other tracking devices: the Council of State issues its decision on the CNIL guidelines
29 June 2020

In its decision of 19 June 2020, the Council of State (Conseil d'État) essentially validated the guidelines on cookies and tracking devices adopted by the CNIL on 4 July 2019. The purpose of these guidelines was to clarify the enhanced legal requirements for internet users.

GDPR. However, the Council of State overturned the provision of the guidelines prohibiting in a general and absolute manner the practice of "cookie walls", ruling that such a prohibition could not be included in an act of soft law. The CNIL takes note of this decision and will adjust its guidelines and future recommendations to comply with it accordingly.





pay or okay


aa) Making access to website content provided without direct monetary payment dependent on the consent of the end-user to the storage and reading of cookies for additional purpose would normally not be considered as depriving the end-user of a genuine choice if the end-user is able to choose between services, on the basis of clear, precise and user-friendly information about the purposes of cookies and similar techniques, between an offer that includes consenting to the use of cookies for additional purposes on the one hand, and an equivalent offer by the same provider that does not involve consenting to data use for additional purposes, on the other hand. Conversely, in some cases, making access to website content dependent on consent to the use of such cookies may be considered, in the presence of a clear imbalance between the end-user and the service provider as depriving the end-user of a genuine choice. This would normally be the case for websites providing certain services, such as those provided by public authorities. Similarly, such imbalance could exist where the end-user has only few or no alternatives to the service, and thus has no real choice as to the usage of cookies for instance in case of service providers in a dominant position.

Article 8

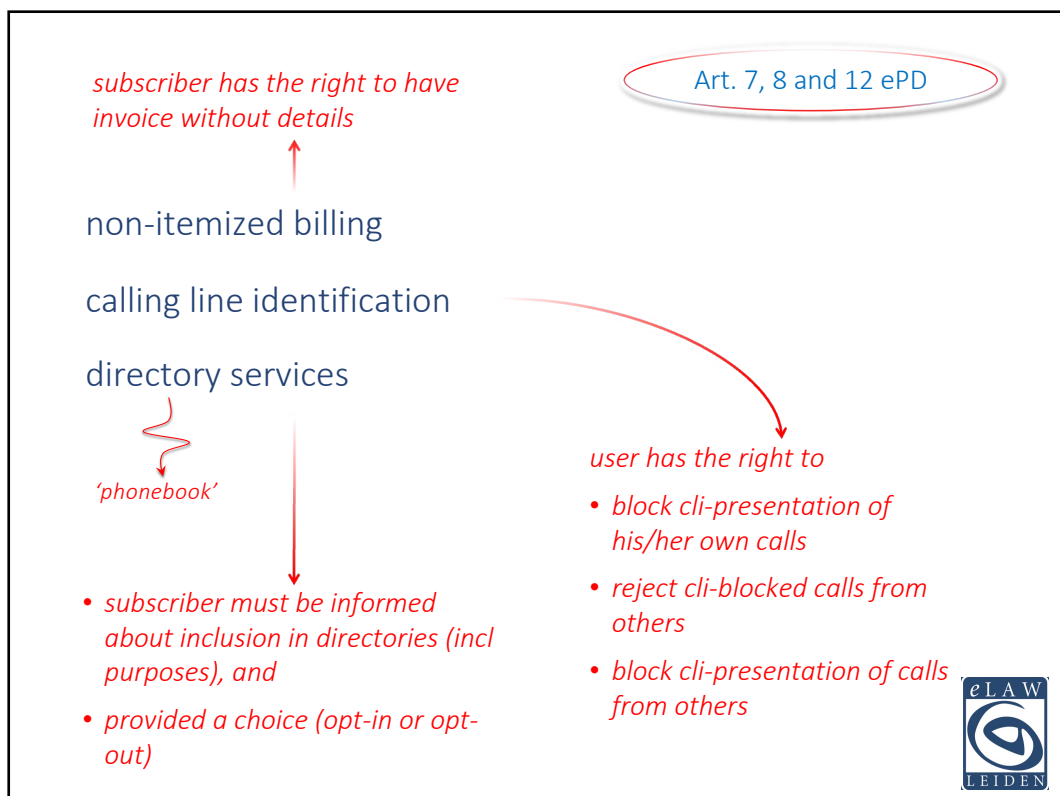
Protection of end-users' terminal equipment information stored in terminal equipment of end-users and related to or processed by or emitted by end-users' terminal such equipment

1. The use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, including about its software and hardware, other than by the end-user concerned shall be prohibited, except on the following grounds:

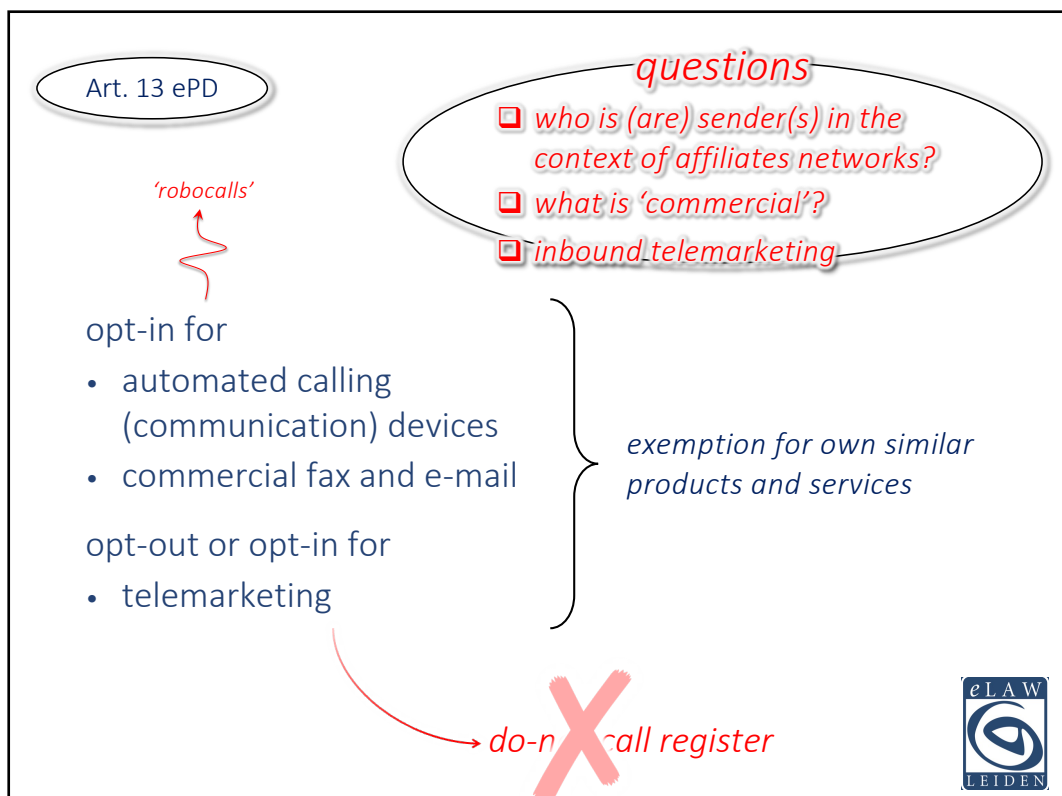
(g1) it is necessary for a purpose other than that for which the information have been collected under this Regulation. Where it is not based on the end-user's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 11 the person using processing and storage capabilities or collecting information processed by or emitted by or stored in the end-users' terminal equipment shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the electronic communications data are initially collected, take into account, inter alia:



communication without identification



unsolicited commercial communication



questions?

g.j.zwenne@law.leidenuniv.nl

