Brussels, 13 July 2018

Dear Member of WP TELE,

The undersigned wish to communicate our common concerns regarding the Austrian Presidency's amendments to the ePrivacy proposal in the text of 10 July 2018 (Council document 10975/18).

Sensitive metadata to be further processed for "compatible purposes" - Articles 6 (2a) and 6 (2aa)

Based on Article 6(4) of the GDPR, the Presidency proposes in Articles 6 (2a) and 6 (2aa) a general provision on permitted the further processing of electronic communications metadata for compatible purposes. Despite the proposed mandatory safeguards (pseudonymisation, restrictions on profiling and prior consultation with the DPA), this significant change undermines the protection of the sensitive data that metadata contains.

With this new change, metadata could be used for any purpose that satisfies the compatibility test and any metadata collected by the electonic communications services provider would fall under this scope. This creates considerable risk for end-users. As Article 6 refers to "processing" and not "collecting", even metadata that is merely automatically generated and processed in the context of providing the electronic communications service, such as destination IP-address for routing of IP packets, may be within the scope of Articles 6(2a) and 6(2aa). Electronic communications metadata in itself constitutes a profile of the end-user's social graph (call detail records), movement patterns (location data) or internet activity. Article 6(2a) will lead to additional storage of such data, with the inherent risk that the data could be leaked through data breaches. Pseudonymisation will generally not prevent re-identification, since most end-users will be unique due to the sheer amount and detail of the data. Moreover, since law enforcement officers can obtain access to the stored metadata, Article 6(2a) will create a de facto blanket and indiscriminate data retention regime similar to the one struck out by the CJEU.

We therefore **oppose these modifications and call for the deletion of the new Article 6 (2a)**.

A vague legitimate interest as a legal basis to process sensitive data - Article 6 (2a)

Article 6(2a) comes very close to introducing a "legitimate interest" legal basis to allow for the further processing of metadata, given its broad and vague language. This fails to recognise that electronic communications metadata reveals very intimate details of individuals and is comparable to sensitive personal data under the case law of the CJEU. In Council document 6726/18 of 7 March 2018, the Bulgarian Presidency specifically noted that it is highly doubtful whether a non-specific provision for permitted processing would, given the sensitive nature of the data involved, be in line with the case-law of the CJEU. It is evident that legitimate interest is not available as legal basis for processing sensitive personal data under the GDPR. Therefore, such an unclear proposal risks therefore

undermining the EU data protection acquis and fails to respect the *lex specialis* nature of the ePrivacy Regulation.

By allowing a vague "legitimate interest" to be used as a legal basis, any restricted approach to further processing of sensitive data is broken and promises of protection of confidentiality of communication become aspirational rather than based on clear legal protections.

Therefore, **we strongly encourage WP TELE to restrict further processing of metadata only to statistical counting based on location data with a short retention period (24 hours) to minimise data protection risks for end-users**. This would still allow further processing for relevant "smart city" purposes and traffic planning in the interest of society.

Tracking walls (recital 20)

Proposed wording in recital 20 would authorise tracking walls for websites without direct monetary payment. This would be allowed in particular if a payment option is available that does not involve access to the terminal equipment ("trackers or other unique identifiers") for purposes not necessary for provision of the service (website).

This change means in practice monetisation of fundamental rights by making personal data a commodity with which EU citizens can "freely" trade albeit without any way of being clearly able to assess the cost. EU citizens will be forced to decide whether to pay for access with money or by being profiled, tracked and abandoning a *fundamental* right. This inherently contradicts, and would result in the lower the level of protection granted under, the GDPR . In fact, Article 7 (4) and recital 52 of the GDPR are clear that " 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."

In this connection, we note that the European Data Protection Board (EDPB) in its guidance on consent under the GDPR (WP 259.rev01) emphasises that Article 7(4) "ensures that the processing of personal data for which consent is sought cannot become directly or indirectly the counter-performance of a contract." Recital 20 allows consent to tracking as counter-performance for visiting a website.

The EDPB also emphasises that consent cannot be regarded as freely given "in cases where there is any element of compulsion, pressure or inability to exercise free will." This must include cases where the end-user has to choose between consent to tracking and expensive subscription options.

We recommend that WP Tele rejects the proposed language in Recital 20.

Deletion of provisions on privacy by design and by default (Article 10)

Astonishingly, the Presidency proposes to delete the key provisions that establish the principle of privacy by design and by default (privacy settings) in Article 10. The alleged rationale is to reduce the burden for browsers and apps and the issue of consent fatigue for

end-users; the consequence in practice will be that technology can be set to track and invade individuals' confidential communications by design and by default with no consequences for companies designing products that fail to respect privacy standards.

We wholeheartly oppose the elimination of such a fundamental measure in the ePrivacy Regulation. Article 10 empowers end-user to be protected by default and to make a decision about privacy settings when the software is installed, supplemented with a periodic reminder.

Technical solutions, such as genuine privacy by design requirements and innovative ways to give or refuse consent, like a mandatory Do Not Track (DNT) standard, are needed to reduce the number of consent requests in the online environment.

The importance of strengthening the provision of Article 10 has been repeatedly stressed by the EDPS and the EDPB, as well as by the LIBE Committee. The proposed deletion of Article 10 would take away any guarantee that end-users will even be able to be sure that technology is secure and protected by design and by default. The recent Cambridge Analytica scandal should remind the EU legislators of the often highly undesirable consequences of data disclosures to unknown third parties.

We strongly recommend that the WP Tele rejects the proposal to delete Article 10 and instead consider ways to strengthen the European Commission text by introducing genuine privacy by design and by default in the ePrivacy Regulation as proposed by the European Parliament, the European Data Protection Board and the European Data Protection Supervisor.

In conclusion, **we count on the Council to reconsider these latest proposals and to swiftly conclude a general approach on the ePrivacy Regulation**, which should deliver a high level of protection for individual's privacy and confidentiality of communications, thereby promoting fundamental rights, trust, innovation and competition.

Yours faithfully,

EDRi

European Digital Rights

accessnow

Access Now

PRIVACY INTERNATIONAL

Privacy International

§@

IT-Political Association of Denmark