European DIGITAL SME Alliance

Position paper on the e-Privacy Regulation Proposal

September 2021

Introduction

The e-Privacy directive and the General Data Protection Regulation (GDPR) are the two legal acts that directly regulate privacy in the EU. Whereas the GDPR applies to all data, e-Privacy specifically regulates electronic communications services within the EU and it is the *lex specialis* to the GDPR when it comes to communications.

Initially, an updated e-Privacy regulation was intended to enter into force in 2018. However, the legislators in the European Parliament and the Council of the EU have so far failed to reach a common agreement.[1] The current comprise proposal put forward by the Portuguese Presidency[2] seems to be falling behind some of the high privacy and data protection provisions set by GDPR. The current proposal allows for the collection of private data via so-called "metadata", which includes individual's browsing history, location at every minute, and with whom an individual interacts and when. While this causes concerns in terms of fundamental rights protection, it is not only a concern for citizens, but also for businesses.

Without consistency between both regulations, Europe risks 1) loosing its unique selling point as a continent that takes privacy & data protection seriously, 2) creating confusion in the market as rules are not aligned, 3) creating mistrust among citizens that count on the protection of their private data. Mistrust and uncertainty could put Europe's sustainable digitalisation at risk.

[1] The privacy-friendly European Parliament's amendments from 2017 have seen resistance in the Council. May/June 2021, the compromise proposed by Germany in November 2020 failed. Earlier this year, the Portuguese Presidency of the EU Council of Ministers presented a new draft version of the e-Privacy regulation[1]. However, some concerns over whether it is well-aligned with the General Data Protection Regulation (GDPR) remain.

[2] https://www.consilium.europa.eu/en/press/press-releases/2021/02/10/confidentiality-of-electronic-communications-council-agrees-its-position-on-eprivacy-rules

+32 2893 0235
VAT: BE0899786252
https://digitalsme.eu
office@digitalsme.eu
Rue Marie Thérèse 21, 1000 Brussels, Belgium
EU Transparency Reg.: 082698126468-52

DIGITAL SME generally welcomes the e-Privacy regulation, and believes that it can complement the GDPR to achieve a level playing field between telecommunication services and internet-based services. However, it should not provide for lower protection than the GDPR.

Main DIGITAL SME comments

- Ensure consistency without a race to the bottom: The e-Privacy regulation should not provide for lower levels of privacy and data protection than the GDPR.
- Protect metadata: With the right to store non-anonymous information for statistical purposes, every single app and web service provider will be able to access people's personal information and store it for an indefinite period of time. This should not be the default option, but users should have to explicitly agree to this, without being able to be excluded from certain services by not agreeing to sharing this private data.
- While regulating cookies has been identified as highly important to ensure higher privacy protection, this technology is already being replaced by so-called "fingerprinting technology" and others. "Fingerprinting" describes a process that identifies an individual by collecting the unique combination of computer settings from the web browser. This information is stored in an online database controlled by the tracking company and no longer on the end user device, such as a personal computer or phone. Storing the identifying data in such databases will decrease the user's control of their personal data, as they can no longer rely on protecting their privacy by configuring their devices' storage through mechanisms such as cookie settings, clearing of cookies and configuring storage security. The regulation needs to give increased legal protection for personal data in order to offer equivalent control to the user.
- Strong privacy provisions are needed to ensure that people will be willing to share data for societal and economic benefits in the future. Some privacy-protective techniques remove private data completely from access – and this is where user-demand may lead us if the e-Privacy regulation does not provide for strong levels of protection. Once removed from the open internet, such data will not be available for anonymised use for the public good and to help transition to a sustainable digital economy and society.

Detailed comments on Portuguese compromise proposal

The importance of protecting metadata

Metadata[3] has just as high a privacy value as the content of a physical letter and must, under the existing e-Privacy regulation, be anonymized or deleted if users do not give their consent. The public opinion on this has also been well studied in several academic studies. A Eurobarometer survey on e-Privacy from 2016 revealed that 70% of Europeans are concerned about how companies use their data. 74% of respondents want to be asked to give consent before their information is collected and processed.[4]

The new Portuguese proposal from the Council now proposes that a communication owner will have the right to save and store metadata for statistical purposes. The problem is that a statistical purpose can be interpreted very broadly. If, for example, a communication provider considers it useful to perform a 20-year study on changes in user behaviour, the communication owner is allowed to save individual profiles on every individual in their system for 20 years. What this means is that all web services will be able to track and build profiles of all people using unique fingerprints of your device, as long as the profiling does not obviously take place for explicitly forbidden purposes such as individual marketing. Likewise, Wi-Fi providers and telecoms may build individual profiles that track your every movement from childhood to old age.

Larger companies like to say that they have the proper security measures in place to protect personal data (despite regular data leaks appearing nonetheless). However, the legislation applies to everyone. Users have, as is set as default in the legislation, consented to share their most sensitive data with large providers and small ones. Access to this data, direct or indirect, may be sold or leaked, and legal loopholes will be exploited to exploint all kinds of secondary uses of users' personal data.

Similar concerns have been raised by the European Data Protection Board (EDPB) in its Declaration on the e-Privacy Regulation (adopted on March 9, 2021). According to

[3] Metadata includes all data surrounding a digital message or call, i.e., who an individual calls or communicates with, the location data and time and duration. Less intuitively, metadata is also the position of an individual's phone every minute of every day and each website that is visited. Using 5G positioning, the positioning accuracy can get in some cases get down to centimeters in the near future.

[4] https://ec.europa.eu/digital-single-market/en/news/eurobarometer-eprivacy

the EDPB some provisions, such as art. 6 letters e) and f), could allow for very broad type of exceptions to the general prohibition of processing metadata. It would therefore be appropriate to further limit these cases, introducing more defined purposes into the Regulation, in order to avoid excessively discretionary interpretations of the norm.[5]

Cookies are irrelevant

Much of the bill's focus is also on regulating cookies. In fact, regulating cookies is starting to become meaningless as they are gradually being replaced by fingerprinting technology. Fingerprinting uses unique user settings to store the same data about your web history as cookies, but on the server side and far away from your browser's control.

With the right to store non-anonymous information for statistical reasons, every single app and web service provider will still be able to access people's personal information and store it for an indefinite period of time. An individual can no longer use, for example, a cookie blocker, and would instead need to invest his own time in each of the countless companies to actively opt out of all such data collection.

In this context, it is important to raise awareness about the role of increasingly common tracking tools, such as browser fingerprinting and other identifiers such as the so-called "MAID" (Mobile Advertising ID), the most common of which are the "IDFA" (Identifier for Advertising, for Apple devices) and the "GAID" (Google Advertising ID, for Android devices). More space should be given also to browsers' implementation of new solutions, through the adoption of a Privacy Sandbox, as from the proposal of FLoC technology (Federated Learning of Cohorts) or from FLEDGE, which involves the use of a "trusted server" to store information regarding advertising campaigns.[6]

[5] Assintel, Parere relativo alla proposta di Regolamento ePrivacy. A cura del GdL Cybersecurity Assintel– Luglio 2021.
[6] See: Assintel, Parere relativo alla proposta di Regolamento ePrivacy. A cura del GdL Cybersecurity Assintel– Luglio 2021.

The best of both worlds: Privacy & data availability

In various surveys[7][8][9], a vast majority of the EU's population desire to say no to all uses of personal data, unless they either give their consent or have guarantees that the data is immediately anonymized. People are highly concerned about their privacy and will look for other solutions if they feel abused. New tools and markets for protecting your data will emerge.

Several examples of such alternatives are already on the market. Apple has, among other initiatives, restricted data collection and randomised Wi-Fi identities. On the web, the privacy-friendly browser Brave and the non-tracking search engine DuckDuckGo are growing in users. We also see increasing use of Tor and other VPN services to completely mask all internet-based communication.

However, once removed from the open internet by privacy protection, data can no longer be used for the common good despite its anonymisation. With the current version of the e-Privacy regulation, we are thus risking the disadvantages of both approaches: we lose the privacy of all citizens as well as the public good enabled by our collective data.

Instead of going down this road of removing valuable data from the open internet for reasons of privacy & data protection, we need a framework that guarantees users high standards of protection, e.g., by promoting and prescribing effective tools and mechanisms to ensure privacy, such as anonymisation, and by guaranteeing a strong legal framework. This way, we can move to the best of both worlds: privacy & data availability for the common good.

[7] Flash Eurobarometer 443: e-Privacy (2016): Q2 “How important for you is each of the following things?”.
[8] Public Attitudes to Data Sharing in Northern Ireland: Findings from the 2015 Northern Ireland Life and Times survey." (2018).
[9] Snijders, D., M. Biesiot, G. Munnichs, R. van Est, with the assistance of Stef van Ool and Ruben Akse (2020). Citizens and sensors – Eight rules for using sensors to promote security and quality of life. The Hague: Rathenau Instituut.

Main contributors

Main contributors: Leonard Johard, Director at Brilliance Center B.V. & CTO at Indivd AB and Assintel's Cybersecurity Working Group.

For further information on this position paper, please contact:

Ms. Annika Linck, Senior EU Policy Manager

E-Mail: a.linck@digitalsme.eu

About European DIGITAL SME Alliance:

European DIGITAL SME Alliance (DIGITAL SME) is the largest network of small and medium sized enterprises (SMEs) in the ICT sector in Europe, connecting about 45,000 digital SMEs. The Alliance is the joint effort of 30 national and regional SME associations from EU member states and neighbouring countries to put digital SME at the centre of the EU agenda.