The Consumer Voice in Europe

PROPOSAL FOR A REGULATION ON PRIVACY AND ELECTRONIC COMMUNICATIONS (E-PRIVACY)

BEUC POSITION PAPER

Contact: David Martin – digital@beuc.eu

BUREAU EUROPÉEN DES UNIONS DE CONSOMMATEURS AISBL | DER EUROPÄISCHE VERBRAUCHERVERBAND
Rue d'Arlon 80, B-1040 Brussels • Tel. +32 (0)2 743 15 90 • www.twitter.com/beuc • consumers@beuc.eu • www.beuc.eu
EC register for interest representatives: identification number 9505781573-45

Co-funded by the European Union

Ref: BEUC-X-2017-059 – 09/06/2017

Why it matters to consumers

The digital revolution has brought enormous benefits to consumers, but it has also created significant challenges for the protection of their privacy. A robust legal framework that protects consumers' fundamental rights to privacy and data protection is necessary to ensure that they can safely benefit from the Digital Economy and trust online services. The e-Privacy rules specifically protect the confidentiality of communications and ensure the protection of consumers' devices (e.g. smartphones and computers) against unwanted intrusions. Moreover, they are essential to guarantee that consumers' online activities cannot be monitored without their permission.

Summary

BEUC welcomes the Commission proposal for a Regulation on Privacy and Electronic Communications ("e-Privacy Regulation"). It shall complement the General Data Protection Regulation ("GDPR") and help create a comprehensive legal framework for the protection of consumers' privacy in a digitised society. Such protections are key to increase consumer trust in this area.

BEUC specifically welcomes that so-called Over-the-Top services (OTTs) are included in the scope, the new enforcement framework and the fact that user consent remains the keystone when it comes to processing electronic communications data, the protection of end-users' devices and to unsolicited communications. We also welcome the aim to better protect consumers against unwanted monitoring of their online behaviour and activities. This is done while also aiming to reduce the number of consent requests encountered by users.

However, there are also several elements in the proposal that raise serious concerns and should be improved during the legislative process. Some provisions may undermine the level of protection granted by the GDPR. In particular:

- BEUC is strongly disappointed by the lack of 'privacy by default' obligations which would ensure that the default settings of smart devices and software are configured to guarantee the highest level of privacy protection from the outset. Article 10 of the proposal should be amended to guarantee such 'privacy by default'.
- We are also very concerned by the fact that the proposed Regulation would allow the possibility to track the physical location and movements of users without asking for their consent. Article 8.2 (b) should be amended so that consent also becomes the general rule for the collection of information emitted by terminal equipment to enable it to connect to another device or to network equipment.
- The proposal also lacks a provision on the representation of users by NGOs and collective redress. This is necessary to ensure a comprehensive enforcement and redress framework for users. A specific provision about the representation of end users, similar to Article 80 of the GDPR, should be included in Chapter V of the

proposal. Otherwise, Article 21 of the proposal should be amended to include a reference to Article 80 of the GDPR.

- There are no specific provisions in the proposed Regulation to safeguard the privacy of children. As recognised by the GDPR, children and young people are vulnerable users that deserve special protection. There should be specific limitations and protection regarding the use of children's communications data and terminal equipment and software made for children.

1. Why we need the e-Privacy Regulation

BEUC welcomes the Commission proposal for a Regulation on Privacy and Electronic Communications[1] ("e-Privacy Regulation"). This Regulation, which shall replace the existing e-Privacy Directive[2], is a fundamental instrument to protect consumer's privacy in the Digital Age. It shall complement the General Data Protection Regulation[3] ("GDPR") and help create a comprehensive legal framework for the protection of consumers' privacy in the digital environment, a key element to increase consumer trust in this area.

Two distinct legal instruments for two distinct fundamental rights

Currently the e-Privacy Directive is the main legal instrument that crystallises Article 7 of the European Charter of Fundamental Rights[4] (the respect for private life) into secondary EU law and specifically protects the confidentiality of communications.

The GDPR on the other hand is built on and enacts Article 8 of the European Charter of Fundamental Rights (the protection of personal data). Its adoption does not change this situation, nor does it eliminate the need for a separate e-Privacy instrument.

The proposed e-Privacy Regulation shall protect privacy and the 'confidentiality of communications'. This is related but different from the protection of 'personal data', which is the aim of the GDPR. Consumers' private spheres and communications must be respected and protected from unwanted intrusions or interferences, regardless of whether personal data are involved or not.

Respect for private and family life

Everyone has the right to respect for his or her private and family life, home and communications.

Article 7 - European Charter of Fundamental Rights

A necessary additional layer of protection

The proposed e-Privacy Regulation would bring an additional layer of protection, complementing the GDPR. Technology has changed the way consumers communicate with each other, the way they interact with businesses and the way they consume goods and services. Continuous digital tracking and analysis of consumers' every move has become the norm. E-Privacy legislation is more necessary than ever before, given the increasingly challenging privacy risks of the Digital Age.

[1] https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications
[2] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0058:20091219:EN:HTML
[3] http://eur-lex.europa.eu/eli/reg/2016/679/oj
[4] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

The GDPR formulates the general framework applicable to the processing and use of personal data in the EU. However, due to the risks and specificities of the electronic communications sector and the online environment, specific rules are justified and necessary, not only for traditional telecommunications services but also for so called Over-the-top communication services ("OTTs"), such as Skype and WhatsApp, that function over the internet and, more broadly, other internet services in general (so-called information society services).

The reasons that led to the adoption of the original e-Privacy Directive in 2002 are still valid and the need to have e-Privacy rules is amplified by the continuous digitisation of society. The proposed e-Privacy Regulation shall particularise and complement the GDPR, in the same way the existing e-Privacy Directive did with the 1995 Data Protection Directive.

For example, without e-Privacy legislation it could be possible to monitor the online activities of consumers and access or retrieve information from their computers and smartphones without asking for their permission, as neither the 1995 Data Protection Directive nor the GDPR specifically require 'user consent' for these actions.

It would also be possible for a company to send marketing messages via email to consumers without asking them first whether they want to receive such messages. This is because the 1995 Data Protection Directive and the GDPR simply establish the basic rule that a consumer has the right to object to the processing of data for marketing purposes, i.e. to get the company to stop sending the marketing messages. They do not require the consumer to 'opt-in' to receive the marketing messages – something the current e-Privacy law does.

The GDPR is a milestone for data protection and will bring major benefits for consumers. It will modernise the data protection framework and adjust it to the new digital environment. But the all-encompassing horizontal nature of the GDPR also means that its rules stay on a general level, establishing the baseline principles and obligations for all market operators. The proposed e-Privacy Regulation aims to go a step further to both complement and build on the solid foundations laid by the GDPR, considering the particularities and privacy risks inherent to the digital communications sector and the online world.

Together with the GDPR, the e-Privacy Regulation shall bring tangible benefits to consumers and help ensure that data-driven innovation and the Digital Single Market thrive in a way that is respectful of citizens' fundamental rights and freedoms.

The e-Privacy Regulation adds a necessary additional layer of protection, particularising and complementing the GDPR.

2. BEUC Position and Recommendations

BEUC welcomes the Commission's proposal. It contains many positive elements, including:

- The choice of regulatory instrument, a Regulation instead of a Directive, which shall bring much needed harmonisation in this area and ensure consistency with the GDPR.

- The extension of the scope to cover OTT services and machine-to-machine communications.
- The fact that 'user consent' remains the key requirement when it comes to processing electronic communications data, as well as in relation to the protection of end-users' devices and to unsolicited communications.
- The broad reach and formulation of the protection of end-users' terminal equipment, which shall better protect consumers against all types of tracking mechanisms. This is done while also aiming to reduce the number of consent requests encountered by users through the inclusion of new targeted exceptions for purposes that should not pose privacy risks (e.g. first party web analytics).
- The new enforcement framework, which follows the approach of the GDPR. There is an alignment between the two instruments in terms of fines and the competence of enforcing the e-Privacy rules is newly mandated exclusively to the Data Protection Authorities.

There are also several elements in the proposal that raise serious concerns which should be improved during the legislative process. Furthermore, some provisions may undermine the level of protection granted by the GDPR. In particular:

- BEUC is strongly disappointed by the lack of 'privacy by default' obligations which would ensure that the default settings of smart devices and software are configured to guarantee the highest level of privacy by protection from the outset.
- We are also very concerned by the fact that the proposed Regulation would allow the possibility to track the physical location and movements of users without asking for their consent.
- The proposal also lacks a provision on the representation of users by NGOs and collective redress. This is necessary to ensure a comprehensive enforcement and redress framework for users.
- There are no specific privacy protections for children.

BEUC's position and recommendations on the main elements of the proposal are further detailed below. Most of our concerns and recommendations are in line with those put forward by the Article 29 Working Party[5] and the European Data Protection Supervisor[6] in their respective opinions.

2.1. Scope and Definitions

Material and Territorial Scope

BEUC supports the material and territorial scope of the proposed e-Privacy Regulation as defined in Articles 2 and 3 of the proposal. The e-Privacy rules shall apply not only to traditional telecommunication services but also to online communication services (like Skype, Viber, Facebook Messenger or WhatsApp) and to machine-to-machine communications in the framework of the Internet of Things. They shall also protect end-users in the EU, regardless of whether the service provider is established in the Union and irrespective of whether a payment is required from the end-user.

The emergence of OTTs and other digital communication services, has exposed limitations and gaps in the current rules. These new services are very popular among European consumers but they currently fall outside the scope of the existing e-Privacy Directive. This

[5] Article 29 Working Party Opinion 01/2017
[6] EDPS Opinion 6/2017

means for example that a consumer sending a message over an OTT service such as WhatsApp does not enjoy the same legal protection as when sending an SMS over a traditional telecoms operator. Consumers are not aware and do not understand these differences in protection. To fill in this gap, it is essential that the e-Privacy Regulation also applies to OTTs.

BEUC also welcomes that the proposed Regulation would apply to wireless networks accessible to anyone in public and semi-private spaces such as Wi-Fi hotspots in cafes, shops and airports. Consumers are increasingly relying on this type of networks and it is important that they are equally protected when using them.

Definitions

Article 4 of the proposal contains the applicable definitions. For the main definitions, including what is considered an 'electronic communication service', the draft e-Privacy Regulation relies on the proposed European Electronic Communications Code[7] (EECC). BEUC considers this to be a valid approach. However, the EECC is still under discussion and the definitions it contains could be amended during the legislative process. Therefore, if the reference to the EECC is to be maintained and no specific definitions are introduced in the e-Privacy Regulation, it is essential to ensure that OTTs are duly covered by the definitions and scope of the EECC.

There is in fact already one important point where the proposed e-Privacy Regulation deviates from the EECC, the definition of "interpersonal communications service". The e-Privacy proposal states that 'interpersonal communications service' shall include services which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service (e.g. instant messaging features within a game, where players can directly communicate). BEUC supports the inclusion of these 'ancillary' communication features in the e-Privacy Regulation. This means that consumers using these communication channels will also be protected by the principle of confidentiality of communications. In the proposed EECC on the other hand ancillary communication features are excluded from the scope.

However, we are concerned by the fact that certain areas of social networks could still fall outside the definition of "interpersonal communications service", even if they allow interactive communication among a limited number of people. This would be the case for example of a 'private' post made by a user on his/her Facebook Timeline to a closed group of people. These situations should also be covered by the Regulation.

Another point of concern relates to the definitions of "metadata" and "location data". According to Article 4 (c) and Recital 17 of the proposed Regulation, location data generated other than in the context of providing electronic communications services should not be considered as metadata. BEUC considers that this exception is unclear and unjustified. Consent should be required as a rule to process location data.

Aggregation of location data can provide a very detailed picture of an individual's life. Where a person lives and works, his/her daily routine, acquaintances, favourite places, etc. The privacy risks are evident regardless of the context in which the location data is generated and regardless of whether it is an online mapping service, a transport planning app or a telecom company using the data. With smartphones and mobile devices, location based services are becoming more and more predominant. GPS location data and Wi-Fi network location data used by information society services in mobile devices is even more

[7] https://ec.europa.eu/digital-single-market/en/news/proposed-directive-establishing-european-electronic-communications-code

accurate than traffic and location data collected by telecoms providers. Therefore, these services should also be required to ask users for consent to access and use their location data. It might be that these services would indeed be required to ask for consent under Article 8 of the proposal but this should be clarified and same conditions should apply regardless of how the location data is generated.

In terms of the definition of 'metadata' as such, there are doubts as to whether the proposed definition clearly comprises metadata generated in the course of the provision of an OTT service.

BEUC Recommendations

- *Ensure that OTT services are duly covered in the definitions contained in the European Electronic Communications Code.*
- *Ensure that the definition of "interpersonal communication services" also includes social networks to the extent that they are used to communicate and interact privately with a limited group of people.*
- *Always consider "location data" as "metadata" and consequently, consent shall be generally required for its processing under Article 6.2 (c). Otherwise, clarify that consent shall be required for the processing of location data by information society services under Article 8.1.*
- *Clarify that the definition of "metadata" (Article 4.3 (c)) also comprises the data generated in the course of the provision of an OTT service.*
- *Ensure that Article 2 covers software providers and persons that use electronic communications services for the purposes of sending direct marketing communications.*

2.2. Confidentiality of Communications

BEUC supports that the principle of confidentiality of communications established in Article 5 of the proposal applies to all electronic communications services, be it traditional telecoms services or OTT services, and that it protects both the content of a consumers' communications (e.g. what is written in an email or said during a phone call) and its associated metadata.

92% of respondents say that it is important that the confidentiality of their emails and messages is guaranteed

Eurobarometer on e-Privacy (Dec 2016)

All electronic communications data shall be confidential, including machine-to-machine communications. This is one of the central elements of the e-Privacy Regulation and one of the main reasons why this Regulation is necessary, as there is no other specific EU legislation that puts into practice the principle of the confidentiality of electronic communications in line with Article 7 of the European Charter of Fundamental Rights.

At the moment, consumers erroneously believe that the messages they send via email or via instant messaging services are confidential when it is not the case. It is very positive that the proposed e-Privacy Regulation would fix this problem.

Article 6 establishes under which circumstances electronic communications data can be processed and used. BEUC welcomes that end user consent is required when processing communications metadata or communications content for purposes other than the transmission of the communications or technical reasons such as the security of the network, billing or meeting quality of service requirements. However, some improvements are necessary to ensure the highest level of protection for the confidentiality of communications and that, when it comes to allowing the processing of electronic communications data, exceptions for processing such data without consent are as limited as possible.

Firstly, given that communications naturally involve more than one party, when consent is required it should be obtained from all end users concerned. In the proposal, this is the case when it comes to processing communication's content (Article 6.3) but not for metadata (Article 6.2 (c)), the latter only requiring the consent of the individual end-user concerned. Metadata can reveal very sensitive information such as who you call, how often, how long a conversation lasts, your location, etc. It can sometimes tell more about an individual than the contents of his/her communications. Therefore, both content and metadata deserve to be equally protected. To allow companies to provide services explicitly requested by the user, e.g. translation or text-to-speech services, a domestic exception could be introduced for the processing of content and metadata for purely personal purposes of the user him or herself, as suggested by the Article 29 Working Party in its opinion.

71% of respondents say it is unacceptable for companies to share information about them without their permission, even if it helps companies provide new services they may like.

Eurobarometer on e-Privacy (Dec 2016)

Secondly, it must be ensured that the provisions for processing communications data without consent remain firmly limited. It should only be possible for providers to process data under these provisions when it is 'strictly necessary' for the purposes that are specifically contemplated in Article 6. Moreover, a possibility to process data on the basis of the 'legitimate interests' of the provider shall be avoided.

In terms of the validity of consent, we welcome that the rules established by the GDPR would also apply whenever user consent is required under the e-Privacy Regulation (Article 9). It is essential to ensure that the rules of both regulations are fully aligned on this issue. The proposed e-Privacy Regulation opens the possibility for telecoms companies to use communications data for purposes which are in principle not allowed under the current e-Privacy Directive. This increases even further the importance of user-consent and ensuring that such consent is informed and freely given. As indicated in recital 18 of the proposal, the e-Privacy Regulation will apply to services which are essential to consumers and the providers of these services cannot force their customers to the processing of data which is not necessary for the provision of the service.

Finally, as consumers' daily use of digital technology continues to increase and connected devices are set to become ubiquitous in the near future, users should always have the right to secure their networks, equipment and communications with the best available techniques. On the other hand, providers of electronic communication services should be obliged to secure all communications by using the best available techniques to ensure security and confidentiality.

BEUC Recommendations

- *Ensure the application of the principle of confidentiality of communications to all means of electronic communications, including OTTs and machine to machine communications.*
- *Ensure that 'user consent' is the cornerstone requirement for the processing and use of electronic communications data for purposes other than the transmission of the communication or technical purposes such as ensuring the security of the services (Article 6).*
- *Provisions allowing the processing of communications data without user consent under Article 6 shall only be applicable when "strictly necessary" (as opposed to just "necessary"). In this sense, it should be made clear for example that processing communications content for targeted advertising purposes is not possible without consent (Article 6.3 (a)), as it shall be possible to provide services without advertising being targeted.*
- *Avoid introducing additional legal basis for processing electronic communications data. In particular, it should not be allowed that service providers can process communications data based on their 'legitimate interests'. This would create uncertainty and weaken the level of protection, undermining the Regulation's purpose and objectives.*
- *Consent of 'all end users concerned' should also be required for the analysis of metadata under Article 6.2 (c), this should also be subject to a mandatory data protection impact assessment.*
- *Stipulate that users should always have the right to secure their networks, equipment and communications with the best available techniques.*

2.3. Protection of end-users' devices and online tracking

BEUC strongly welcomes that the proposed e-Privacy Regulation seeks to ensure that consumers' activities are not monitored without their permission and that end-user's terminal equipment such as computers and smartphones are protected against unwanted intrusions. It shall not be allowed to track users' behaviour and activities without their knowledge and consent. Moreover, consumers should have the possibility to use online services without being under constant commercial surveillance.

Digital tracking and corporate surveillance on the internet is one of the main problems that consumers are facing today[8]. Extensive tracking and profiling techniques can be (ab)used to discriminate consumers and to influence their behaviour. This can have substantive negative implications for consumers and seriously undermine their fundamental rights and freedoms. This problem is aggravating with the widespread commercial use of Big Data analytics across the board in all types of services and the proliferation of connected devices.

9 out of 10 say it is important that the information on their computers can only be accessed with their permission.

More than 8 out of 10 say tools for monitoring their online activities should only be used with their permission.

Eurobarometer on e-Privacy (Dec 2016)

BEUC welcomes the broad reach and approach of Article 8.1 of the

[8] See "Networks of Control: A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy", by Wolfie Christl and Sarah Spiekermann.

proposed Regulation and the fact that consent is at its core (Article 8.1 (b)). The wording of the article, which refers to the "use of processing and storage capabilities" of terminal equipment in addition to the "collection of information" from such equipment, shall guarantee that any kind of tracking mechanism falls under the scope of the provision, not just 'traditional' tracking tools such as cookies. Recital 20 further acknowledges that tracking should only be allowed with the end-user consent and for specific and transparent purposes.

Targeted advertising is one of the main reasons of the widespread tracking and monitoring practices that consumers are subjected to online. BEUC recognises the importance that advertising has for the funding of internet services and online content. However, we strongly regret that the predominant advertising based business model has been developed at the expense of consumers' privacy, based on 24/7 surveillance and monetisation of consumers' every move by a myriad of entities (advertisers, publishers, advertising networks, ad-exchange platforms, data brokers, etc.) which are completely unknown by the consumer. Most consumers remain oblivious and/or powerless in this situation. Moreover, there is basically no choice but to accept to be tracked if you want access to the service.

A report published by the Norwegian Data Protection Authority in January 2016[9] shows that a large majority of users (73%) would prefer random advertising to targeted advertising (27%). The 2015 Data Protection Eurobarometer[10] also showed that a majority of Europeans are uncomfortable with internet companies using information about their online activity to tailor advertisements.

Consumers' concerns are further confirmed by the Eurobarometer on e-Privacy published by the Commission in December 2016. The e-Privacy Regulation should address this problem, complementing the provisions in the GDPR on the conditions for valid consent. For example, 'tracking walls' should be explicitly prohibited. Users shall not be denied access to a service if they refuse to accept to be tracked for purposes which are not strictly necessary.

74% think it is unacceptable to pay in order not to be monitored when using a website

64% think it is unacceptable to have their online activities monitored in exchange for unrestricted access to a certain website

Eurobarometer on e-Privacy (Dec 2016)

This is not incompatible with services being funded through advertising. First, advertising should not necessarily have to be privacy invasive. Second, nothing prevents those wishing to provide targeted behavioural-based advertising to request and obtain users' consent for this purpose.

As foreseen in Article 8.1, there are also specific cases where consent shall not be required. Like for the processing of electronic communications data under Article 6, it is important that these cases are narrowly defined and can only be used when there is 'strict' necessity.

It is also important that consumers are not faced with constant consent requests. We welcome the introduction of a specific provision regarding 'first party' web audience measuring (Article 8.1 (d)), although what falls under this concept should be further clarified to avoid possible misuse of this provision. Moreover, it must be clear that in the

[9] https://www.datatilsynet.no/globalassets/global/english/privacy-trends-2016.pdf
[10] http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_sum_en.pdf

case of web audience measuring falling under the exception, end users must be able to object to the processing of their data. The principle of data minimisation and the relevant provisions of the GDPR must in any case apply.

The possibility to express consent by using the appropriate technical settings of software enabling access to the internet (Article 9.2) should also help reduce the number of consent requests, as long as service providers do not systematically request separate consent for privacy invasive purposes such as tracking for targeted behavioural-based advertising. In this sense, it is important to remember that, according to the Data Protection Authorities[11], for consent provided via technical settings to be valid, settings cannot be predetermined to accept all cookies in bulk for example. Comprehensive and fully visible information is also necessary to ensure valid consent and it should not be possible to "bypass" the choice made by the user in the settings. On this last point, recital 22 states that the choices made by end-users when establishing the privacy settings of a browser or other application should be binding on, and enforceable against any third parties. We strongly welcome this and recommend that it should also be stated in Article 9.2.

Tracking of physical location and movements of users (Article 8.2)

Article 8.2 (b) is one of our biggest elements of concern in the proposal. It opens the possibility for tracking the physical location and movements of end-users without asking for their consent nor giving them the right to object the data collection. The tracking would be done through the collection of information emitted by terminal equipment to enable it to connect to another device or to network equipment. Only prominent notice with the basic information regarding the process is required, and there are no clear limitations in relation to the scope of the data collection or further processing.

While we acknowledge the useful positive functionalities that the use of this data could have (e.g. providing data on the number of people in a specific area or traffic jams/waiting times), the privacy risks are high and the proposed Regulation fails to provide sufficient safeguards. This Article goes against the essence and objectives of the proposed Regulation and undermines the protection accorded by the GDPR. Recital 25 of the proposal even acknowledges the possible high privacy risks (e.g. tracking of an individual's movements over time) and that the data collected could be used for intrusive purposes (e.g. to send commercial messages to consumers as they walk by or enter a store).

BEUC Recommendations

- *Ensure strong protection of end-users against intrusions or interferences in their technical equipment and against online tracking.*
- *Consent shall de facto remain the default requirement. The exceptions under Article 8.1 (a), (c) and (d) that permit interfering with end-users' terminal equipment without consent should only be used when "strictly necessary" (as opposed to just "necessary").*
- *Explicitly ban 'tracking walls' which oblige users to consent to the monitoring of their activities in exchange for unrestricted access to a certain website.*
- *Clarify the meaning of the last sentence of Recital 21 in relation to the use of 'anti-tracking tools' by end-users. The use by service providers of mechanisms to disable or circumvent 'anti-tracking tools' without prior consent from end-users' should be prohibited.*

[11] See Article 29 Working Party Opinion WP141 on Behavioral Advertising.

- *End-users should have the right to protect their IT-systems against unlawful intrusions. They should have the right to protect their communication and to protect their systems, for example against malvertising[12]. It should be not allowed to circumvent such security measures.*
- *Indicate in Article 9.2 that the choices made by end-users when establishing the privacy settings of a software application or a device should be binding on and enforceable against any third parties.*
- *Clarify the concept of "web audience measuring" (Article 8.1 (d)) to avoid misuses.*
- *Ensure that Article 9.3 on the withdrawal of consent, also applies to the protection of end-users' terminal equipment (Article 8.1 (b)).*
- *Substantially amend Article 8.2 (b) so that consent also becomes the general rule for the collection of information emitted by terminal equipment to enable it to connect to another device or to network equipment. Exceptions to this rule should be narrowly defined, allowed only for cases where there is a low privacy risk. They should mostly focus on the use of these data in an anonymised manner for public interest/utility purposes. In this sense, it should be mandatory to carry out an impact assessment to evaluate the privacy risks of the data collection. Also, when user consent is not required, the user must have in any case the right to opt-out. Generally, it must be clear that all the relevant GDPR principles and provisions apply in addition to these requirements.*

2.4. Privacy by default

A big concern is the lack of "privacy by default" obligations which would ensure that the default settings of smart devices and software are configured to guarantee the highest level of privacy by protection from the outset.

Article 10 of the proposed Regulation only obliges that software permitting electronic communications offers the option to prevent third parties from storing information on the terminal equipment of an end-user or processing information already stored in that equipment. It also requires that, upon installation, the software shall inform the end-user about the privacy setting options and, to continue installation, the end-user must make a choice.

These "choice" obligations are not negative *per se*, but they are not equivalent to "privacy by default", which means that the strictest privacy settings are set on *by default* and automatically apply once a customer starts using a new product or service. As it stands, Article 10 could undermine Article 25 of the GDPR, which establishes the principles of "data protection by design"[13] and "data protection by default"[14]. The e-Privacy Regulation should build upon this article of the GDPR. This is even more important given that the Regulation is 'lex-specialis' to the GDPR. Moreover, the results of the Eurobarometer on e-Privacy[15] were also very clear on this point, showing strong support in favour of 'privacy by default', but this has inexplicably been ignored.

89% agree that the default setting of their browser should stop their information from being shared

Eurobarometer on e-Privacy (Dec 2016)

[12] Use of online advertising to spread malware.
[13] Embedding data protection measures and privacy enhancing technologies directly into the design of information technologies, systems and services.
[14] By default, only personal data which are necessary for each specific purpose of the processing are processed.
[15] http://ec.europa.eu/COMMFrontOffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/76378

Moreover, the scope of the proposed provision seems too narrow. While it refers to "software placed on the market permitting electronic communications", looking at Recitals 22, 23 and 25 the focal point is web browsers. It is necessary to ensure that 'privacy by default' obligations also apply to operating systems and apps, and to any connected device. This is particularly important keeping in mind cross-device tracking technologies.

Also, Article 10 only mentions preventing third parties from storing information or processing information in end-users' terminal equipment. There is no obligation to offer the option to prevent third parties from using the processing capabilities of the terminal equipment. This omission seems at odds with Article 8.1 and due to the fact that terminal equipment itself does not fall under the scope of the current provision, it is only targeted at software.

BEUC Recommendations

- *Introduce a clear and robust 'privacy by default' requirement. The settings of all end-users' devices and software shall be configured to provide the highest level of privacy protection from the outset and prevent tracking of users' activities by third parties.*
- *Clarify that "software permitting electronic communications" also includes operating systems and apps.*

2.5. Unsolicited commercial communications

BEUC welcomes that prior user consent is established as the general requirement for the purposes of delivering direct marketing communications, no matter type of form of the communication.

The wording of Article 16.1 could however be strengthened by establishing a clear prohibition to send direct marketing communications without consent. Also, the use of the word "send" could create uncertainty as to whether it covers certain direct marketing communications which are not technically 'sent' to users, such as targeted ads displayed on websites. This could be solved by using a word such as "serve" so that there is no doubt that all types of direct marketing communications are duly covered. This should also be reflected in the definition of "direct marketing communications" in Article 4.3 (f)."

There is also an issue with Article 16.2 which states that where a natural or legal person obtains electronic contact details for electronic mail from its customer, in the context of the sale of a product or a service, they may use these electronic contact details for direct marketing of their own similar products or services. The problem is that under Article 4.3 (e) electronic mail is defined as "any electronic message containing information such as text, voice, video, sound or image sent over an electronic communications network". This means that Article 16.2 would not only apply to traditional e-mail. Companies could send consumers all kind of messages (text, voice, video, sound or image) without their consent, when they have obtained their electronic contact details in the context of the sale of a product or a service. Therefore, the words "electronic mail" in Article 16.2 should be replaced "e-mail" and, to avoid confusion, Article 4.3 (e) should be amended to replace the term "electronic mail" by a more general term such as "electronic message".

We welcome the increased transparency requirements for direct marketing calls. According to Article 16.3, those placing direct marketing calls shall present the identity of a line on which they can be contacted or a specific code/or prefix identifying the fact that the call is a marketing call. However, presenting these requirements as an alternative option, one or the other, could result in fragmentation and a lower level of consumer protection in some

Member States. Therefore, to ensure a basic harmonised level of protection all across the EU, the presentation of the caller ID should be mandatory while the special pre-fix could remain optional.

The possibility for Member States to establish an opt-out system for voice-to-voice marketing calls is envisaged in Article 16.4. It should be added that Member States choosing to use such a system should be obliged to ensure that there are effective safeguards to guarantee compliance and strong enforcement. It must also be clear what rules apply if a company from a country where there is an opt-out regime calls a consumer in another country where an opt-in system applies.

Finally, it must also be clear that the rules on consent and the right to object of the GDPR also apply in this context. Notably, it shall be as easy to withdraw consent as to give consent and consumers shall have the right to object at any time free of charge.

BEUC Recommendations

- *Strengthen the wording of Article 16.1 by turning it into a straightforward prohibition to send or serve direct marketing communications without prior end-user consent.*
- *Amend the definition of "direct marketing communications" in Article 4.3 (f) and Recital 32 to make sure it also covers commercial communications that are not 'sent' to users in the strict sense of the term (e.g. targeted advertising served or presented to the users in a given website).*
- *In Article 16.2, the words "electronic mail" by should be replaced by "e-mail". Also, to avoid confusion, in Article 4.3 (e) the words "electronic mail" should be replaced by "electronic message".*
- *Amend Article 16.3 to make the presentation of the caller ID mandatory for direct marketing calls, while maintaining the special pre-fix as an option for Member States who might wish to also introduce this requirement*[*]*.*
- *Member States choosing to use an opt-out a system for direct marketing calls should be obliged to ensure that there are effective safeguards to guarantee compliance and strong enforcement.*
- *Article 16.6 should make it clear that, in accordance with the GDPR, it should be as easy to withdraw consent as it was to give it and that end-users have the right to object free of charge.*

2.6. Enforcement and redress

BEUC welcomes that Chapters IV and V of the proposed Regulation mirror the enforcement and redress system under the GDPR and that competence for the enforcement of the e-Privacy Regulation is allocated to the Data Protection Authorities (DPAs).

However, a key element is missing in the proposed Regulation. Article 80 of the GDPR grants data subjects the right to mandate a non-for profit organisation to act on his/her behalf. It also provides the possibility for Member States to allow not-for-profit organisations to take action in their own initiative to defend collective interests in the area of data protection. Both things should also be explicitly allowed under the e-Privacy Regulation.

** Due to the national situation and experience of consumers in France, UFC-Que Choisir asks for stronger measures on direct marketing calls.*

In terms of the fines that the Data Protection Authorities can impose, we consider that breaching the protection of end-users' terminal equipment shall be as serious as breaching the confidentiality of communications. Computers and smartphones are part of consumers' private sphere (Recital 20). The same could be said of a connected car or a smart hub in a home. The information that these devices contain is highly personal and can reveal countless details of an individual's life and character.

Finally, it is also important to foster cooperation between the Data Protection Authorities and enforcement authorities from all relevant sectors, not only telecoms regulators (NRAs). This is key to ensure coherent enforcement.

BEUC Recommendations

- *Introduce a specific provision in Chapter V about the representation of end users, like Article 80 of the GDPR. Alternatively, introduce a reference to Article 80 of the GDPR in Article 21 of the proposal.*
- *Consider non-respect of the obligations related to the protection of end-users' terminal equipment to be as serious as breaching the confidentiality of communications. This would mean deleting Article 23.2 (a) and mentioning Article 8 alongside Articles 5, 6 and 7 in Article 23.3 of the proposal.*
- *Stipulate in Article 18.2 that the DPAs should cooperate not only with the telecoms NRAs but also with other relevant enforcement authorities including, for example, consumer protection authorities.*

2.7. Other issues

Restrictions

BEUC is concerned that Article 11 of the proposed Regulation would expand the possibilities for Member States to restrict the rights of citizens even beyond what is currently allowed in the e-Privacy Directive.

Under Article 15 of the e-Privacy Directive, restrictions are allowed to safeguard national security, defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system. The proposed Regulation would substantially expand the possibilities for Member States to restrict users' rights.

Firstly, the proposed Article 11 would allow Member States to restrict users' rights "to safeguard one or more of the general public interests referred to in Article 23.1 (a) to (e) of the GDPR". This is already broader than what is currently foreseen in the e-Privacy Directive. In particular, Article 21.3 (e) of the GDPR allows restrictions to safeguard "other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest (..)". Secondly, the proposed Article 11 would also allow restrictions for a monitoring, inspection or regulatory function connected to the exercise of official authority for the interests mentioned above. All this seems unjustifiably broad and disproportionate.

Moreover, it must be clear that any legal measure adopted by Member States under this provision should also comply with Article 23.2 of the GDPR and contain specific provisions, among other things, about the purposes of processing, the scope of the restrictions introduced, the safeguards to prevent abuse and the right of end-users to be informed about the restrictions.

Internet of Things

Recital 12 explicitly states that the proposed Regulation applies to machine-to-machine communications. We welcome this explanation and would like to underline how important it is that Internet of Things devices and applications remain within the scope of the Regulation, given the specific challenge they pose in terms of privacy and security.

It is essential that transmission systems that allow for the conveyance of signals by radio remain included in the definition of "communication networks". It is also essential that "electronic communications data" remains defined in a sufficiently broad and technology neutral way, in line with recital 14 of the proposed Regulation.

Children

We consider it necessary to introduce specific provisions in the proposed Regulation to safeguard the privacy of children.

Children and young people are vulnerable users that deserve special protection. For example, a recent campaign carried out by our member organisations in relation to internet connected toys[16] uncovered serious violations of consumer protection and data protection rules and highlighted serious risks related to the privacy and security of children using such toys.

Companies like Google are increasingly offering specific services directly aimed at children (e.g. YouTube for Kids). While these efforts should contribute to a safer environment for younger users and foster their participation in the digital world, there can also be negative implications for children and youth privacy. Using these services means for children that they can become subject to the tracking, profiling and data monetisation practices generally inherent to 'normal' digital services.

Article 8 of the GDPR, which establishes the conditions applicable to child's consent in relation to information society services, is not reflected nor referenced in the proposal. In fact, there are no references to children in the whole text.

There should be specific limitations and protection regarding the use of children's communications data and to terminal equipment and software made for children. Children's communications data should never be used for targeted advertising purposes for example. Also, children should not be targeted by websites using profiling and behavioural marketing techniques.

Calling line identification and publicly available directories

We welcome the protection of the right of the calling party to hide their phone number and the right of the called party to reject calls from unidentified parties (Article 12).

We also welcome the proposed exceptions to the presentation of calling and connected line identification envisaged in Article 13 (e.g. when overriding the elimination of calling line identification is necessary to allow emergency services, such as eCall, to carry out their tasks).

We also support the inclusion of the obligation for number-based interpersonal communication services to provide called end-users with the possibility, free of charge, to

[16] https://www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws/

block incoming calls from specific numbers or anonymous sources and to stop automatic call forwarding by a third party to the users' terminal (Article 14).

With regard to publicly available directories, we welcome the obligation for providers of such directories to obtain users' consent before including their information in a directory (Article 15).

Date of application

We support that, as put forward in the proposal, the Regulation becomes applicable on 25 May 2018, at the same time as the GDPR. This would ensure consistency and legal certainty both for businesses and consumers.

BEUC Recommendations

- *Limit the possibilities for Member States to restrict the rights of citizens under Article 11. These should not go beyond what is currently allowed in Article 15 of the e-Privacy Directive. Also, ensure safeguard and transparency obligations to be respected by Member States that introduce restrictions.*
- *Ensure that machine-to-machine communications duly remain in the scope of the Regulation.*
- *Introduce specific provisions to safeguard the privacy of children and youngsters. There should be special limitations and protections related to the use of children's communications data and to terminal equipment and software made for children. Notably, children's communications data should never be used for targeted advertising purposes. Also, children should not be targeted by websites with children content using profiling and behavioural marketing techniques.*
- *Maintain 25 May 2018 as the date for the Regulation to be effectively applicable, to make it coincide with the application of the GDPR and avoid legal inconsistencies.*

-END

This publication is part of an activity which has received funding under an operating grant from the European Union's Consumer Programme (2014-2020).