**Industry-wide Amendments on the Croatian Presidency's proposal for a Regulation 6543/20 from 6 March 2020**

**Brussels, 18 March 2020**

*Article 8*

*Protection of **end-users' terminal equipment** information ~~stored in and related to end-users' terminal 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:

(a) it is necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network; or

(b) the end-user has given his or her consent.; or

(c) it is necessary for providing ~~an information society~~ service requested by the end-user; or

(d) ~~if~~ it is necessary for ~~web~~ audience measuring, provided that such measurement is carried out by the provider of the ~~***information society***~~ service requested by the end-user **or by a third party, or by third parties jointly, on behalf of ~~the~~ one or more providers of the ~~*information society*~~ service provided that conditions laid down in Article 28, or where applicable Article 26, of Regulation (EU) 2016/679 are met; or**

~~(da) it is necessary to maintain or restore the security of information society services or terminal equipment of the end-user, prevent fraud or detect technical faults for the duration necessary for that purpose; or~~

~~(e) it is necessary for a software update provided that:~~

~~(i) such update is necessary for security reasons and does not in any way change the privacy settings chosen by the end-user are not changed in any way,~~

~~(ii) the end-user is informed in advance each time an update is being installed, and~~

~~(iii) the end-user is given the possibility to postpone or turn off the automatic installation of these updates; or~~

**(f) it is necessary to locate terminal equipment when an end-user makes an emergency communication either to the single European emergency number '112' or a national emergency number, in accordance with Article 13(3).**

**(g) it is necessary for the purpose of the legitimate interests pursued by a service provider to use processing and storage capabilities of terminal equipment or to collect information from an end-user's terminal equipment, except when such interest is overridden by the interests or fundamental rights and freedoms of the end-user.**

**The end-user's interests shall be deemed to override the interests of the service provider where the ~~*end user is a*~~ *service is directly aimed to a* child or ~~where the service provider processes, stores or collects the information to *specifically* determine the nature and characteristics of the *personally identified specific* end-user or to build an individual profile *attributed to of* the end-user or~~ the processing, storage or collection of the information by the service provider contains special categories of personal data as referred to in Article 9(1) of Regulation (EU) 2016/679. Where the service provider processes, stores or collects the information to determine the nature and characteristics of the end-user or to build an individual profile of the end-user , the data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her and shall have the right not to be subject to a decision based solely on automated processing, which produces legal effects concerning him or her or similarly significantly affects him or her in accordance with respectively article 21 and article 22 of Regulation (EU) 2016/679.**

***Justification***

In the digital environment and specifically on the open web, it is difficult to asses whether amongts the readers of a publication which is freely available online there are children. As such, for a more practical approach and more legal certainty for digital players, we suggest that Member States consider the restriction regarding minors, as an alligment with the GDPR, by providing that the minors' interest shall override when the services of the provider are aimed at children as their primary audience.

Furthermore, regarding content providers and their capacity to personalise and adapt their offerings to an individual user by creating user profiles, the GDPR contains the necessary safeguards to ensure that users are sufficently protected, while allowing service providers enough flexibility in order to personalise their offerings. As such, we suggest an alligment with Articles 21 and 22 of the GDPR which ensure user with the same right to object to certain type of processing at any time during the process.

**1a. Service providers using processing and storage capabilities of the end-user's terminal equipment or collecting information from the end-user's terminal equipment pursuant to paragraph 1(g) *~~shall~~ may* share the information with any third party other than its processors, *~~acting in accordance with Article 28 of Regulation (EU) 2016/679 mutatis mutandis, unless it has been made anonymous and~~ provided that appropriate technical and organisational measures such as, but not limited to pseudonymisation and encryption are applied*. Prior to any use of processing or storage facilities in, or collection of information from the end-user's terminal equipment, the service provider shall:**

***Justification***

The requirement to anonymise data before it is shared with third parties, as proposed by the Croatian Presidency, would go further than what the GDPR requires and unduly restrict the use of legitimate interest for the media industry online (e.g. in comparison with the offline world). The inherent limitations to the use of legitimate interest under GDPR, coupled with the additional requirements introduced by this new Regulation (see following subparagraphs (a), (b) and (c)) already provide strong safeguards for users' privacy.

In particular, pseudonomysation and encryption ensure an adequate level of privacy for the user while providing an enforceable solution for service providers that would produce warranted results, while the obligation to carry out a DPIA would ensure that users' rights are duly considered and protected, and that publishers can be held accountable.

**Alternative propsal Art. 8 para 1 a:**

**1a. Service providers using processing and storage capabilities of the end-user's terminal equipment or collecting information from the end-user's terminal equipment pursuant to paragraph 1(g) *~~shall~~ may* share the information with any third party ~~other than its processors~~, *provided that conditions laid down in ~~acting in accordance with~~* Article 28 *or where applicable Article 26,* of Regulation (EU) 2016/679 *are met mutatis mutandis, ~~unless it has been made anonymous~~ and appropriate technical and organisational measures such as, but not limited to, pseudonymisation and encryption are applied*. Prior to any use of processing or storage facilities in, or collection of information from the end-user's terminal equipment, the service provider shall:**

***Justification***

While the reasoning behind our alternative proposal remains the same as for our first proposal. Nonetheless, because Article 26 relates to joint controllership, it could imply substantial challanges in practice for the press sector.

**(a) carry out an assessment of the impact of the use of the processing and storage capabilities or the collection of information from the end-users' terminal equipment and of the envisaged processing on the confidentiality of communications and the privacy of end-users in accordance with Article 35 of Regulation (EU) 2016/679, which may result in the prior consultation of the supervisory authority in accordance with Article 36(1) to (3) of Regulation (EU) 2016/679;**

**(b) inform the end-user of the envisaged processing operations based on paragraph 1(g) and of the end-user's right to object to such processing, free of charge, at any time, and in an easy and effective manner; and**

**c) implement appropriate technical and organsational measures, such as pseudonymisation and encryption.**

***1b. For the purposes of paragraph 1 point (b), consent may be expressed by continuing the use of an information society service, having been provided with***

***clear and comprehensive information that this action by the end-user signifies consent. Access to website content may still be made conditional on the well-informed acceptance of a cookie or similar ~~device~~, technologies if it is used for a legitimate purpose***

***Justification***

It is becoming increasingly clear that the fragmented interpretations of the GDPR by the DPAs in Member States are creating uncertainty for content producers.

As such, we find it necessary to use the opportunity given by the introduction of an ePrivacy Regulation to harmonise the interpretation of consent across MS, in order to acquire MS, the judiciary, bussinesses and consumers with more legal certainty.

Furthermore, the possibility to condition access to services remains of utmost importance to the media sector. We remain concerned with the deletion of any reference to conditionality in recital 20. Conditionality should be acknowledged as a full right for the media sector and therefore placed in the body of the legislation.

2. The collection of information emitted by terminal equipment **of the end-user** to enable it to connect to another device and, or to network equipment shall be prohibited, except ~~if~~ **on the following grounds**:

(a) it is done exclusively in order to, for the time necessary for, and for the purpose of establishing **or maintaining** a connection; or

**(b) the end-user has given his or her consent; or**

**(c) it is necessary for the purpose of statistical counting that is limited in time and space to the extent necessary for this purpose and the data is made anonymous or erased as soon as it is no longer needed for this purpose,**

**(d) it is necessary for providing a service requested by the end-user.**

~~(b)~~**2a. For the purpose of paragraph 2 points (b) and (c),** a clear and prominent notice ~~is~~ **shall be** displayed informing of, at least, the modalities of the collection, its purpose, the person responsible for it and the other information required under Article 13 of Regulation (EU) 2016/679 where personal data are collected, as well as any measure the end-user of the terminal equipment can take to stop or minimise the collection.

**2b.** **For the purpose of paragraph 2 points (b) and (c),** ~~T~~**t**he collection of such information shall be conditional on the application of appropriate technical and organisational measures to ensure a level of security appropriate to the risks, as set out in Article 32 of Regulation (EU) 2016/679, have been applied.

3. The information to be provided pursuant to ~~point (b) of~~ paragraph 2**a** may be provided in combination with standardized icons in order to give a meaningful overview of the collection in an easily visible, intelligible and clearly legible manner.

4. The Commission shall be empowered to adopt delegated acts in accordance with Article 2~~57~~ determining the information to be presented by the standardized icon and the procedures for providing standardized icons.

**(20a) End-users are often requested to provide consent to the storage and access to stored data in their terminal equipment, due to the ubiquitous use of tracking cookies and similar tracking technologies. As a result, end-users may be overloaded with requests to provide consent. This can lead to a situation where consent request information is no longer read and the protection offered by consent is undermined. Implementation of technical means in electronic communications software to provide specific and informed consent through transparent and user-friendly settings, can be useful to address this issue. Where available and technically feasible, an end user may therefore grant, through software settings, consent to a specific provider for the use of processing and storage capabilities of his or her terminal equipment for one or multiple specific purposes across one or more specific services of that provider. For example, an end-user can give consent to the use of certain types of cookies by whitelisting one or several providers for their specified purposes. Providers of software are encouraged to include settings in their software which allows end-users, in a user friendly and transparent manner, to manage consent to the storage and access to stored data in their terminal equipment by easily setting up and amending whitelists and withdrawing consent at any moment.**(21) ~~Exceptions to the obligation to obtain consent to make u~~**U**se of the processing and storage capabilities of terminal equipment or ~~to~~ access **to** information stored in terminal equipment

**without the consent of the end-user** should be limited to situations that involve ~~no,~~ ~~or~~ only very limited, intrusion of privacy. For instance, consent should not be requested for authorizing the technical storage or access which is ~~strictly~~ necessary and proportionate for the ~~legitimate~~ purpose of ~~enabling the use of~~ **providing** a specific service ~~explicitly~~ requested by the end-user. This may include the storing of cookies for the duration of a single established session on a website to keep track of the end-user's input when filling in online forms over several pages**, authentication session cookies used to verify the identity of end-users engaged in online transactions or cookies used to remember items selected by the end-user and placed in shopping basket**. **In the area of IoT services which rely on~~/deploy~~ connected devices (such as connected thermostats, connected medical devices, smart meters or automated and connected vehicles), the use of the processing and storage capacities of those devices and access to information stored therein should not require consent to the extent that such use or access is necessary for the provision of the service requested by the end-user. For example, storing of information in or accessing information from a smart meter might be considered as necessary for the provision of a requested energy supply service to the extent the information stored and accessed is necessary for the stability and security of the energy network or for the billing of the end-users' energy consumption**

**~~In some cases the use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment may also be necessary for providing an information society service, requested by the end-user, such as services provided to safeguard freedom of expression and information including for journalistic purposes, such as online newspaper or other press publications as defined in Article 2(4) of Directive (EU) 2019/790, that is wholly or mainly financed by advertising provided that, in addition, the end-user has been provided with clear, precise and user-friendly information about the purposes of cookies or similar techniques and has accepted such use~~**

**~~To the extent that use is made of processing and storage capabilities of terminal equipment and information from end-users' terminal equipment is collected for other purposes than for what is necessary for the purpose of carrying out the transmission of an electronic communication over an electronic communications network or for the provision of the service requested, consent should be~~**

~~**required. In such a scenario, consent should normally be given by the end-user who requests the service from the provider of the service**~~.

**(21a)** Cookies can also be a legitimate and useful tool, for example, in **assessing the effectiveness of a delivered information society service, for example of website design and advertising or by helping to** measur~~eing web traffic to~~ **the numbers of end-users visiting** a website**, certain pages of a website or the number of end-users of an application. This is not the case, however, regarding cookies and similar identifiers used to determine the nature of who is using the site, which always require the consent of the end-user**. Information society providers that engage in configuration checking to provide the service in compliance with the end-user's settings and the mere logging of the fact that the end-user's device is unable to receive content requested by the end-user should not constitute access to such a device or use of the device processing capabilities.

**(21b) The legitimate interests of a service provider could provide a legal basis to use processing and storage capabilities of terminal equipment or to collect information from an end-user's terminal equipment, provided that such interests are not overridden by the interests or the fundamental rights and freedoms of the end-user, taking into consideration the reasonable expectations of end-user*s*** **based on ~~*her or his*~~ *their* relationship with the provider. The demonstration of a legitimate interest requires careful assessment, in particular whether ~~*an*~~ end-user*s* can reasonably expect that the use of processing and storage capabilities of ~~*her or his*~~ *their* terminal equipment or the collection of information from it, may take place. Only if the results of the balancing test undertaken by the service provider demonstrate that its legitimate interest is not overridden by the interests and the fundamental rights and freedoms of the end-user, can the service provider rely on that legal basis.**

**A legitimate interest could be relied upon where ~~*the*~~ end-user*s* could reasonably expect such storage, processing or collection of information in or from ~~*her or his*~~ *their* terminal equipment in the context of an existing customer relationship with the service provider. For instance, maintaining or restoring the security of information society services or of the end-user's terminal equipment, or**

**preventing fraud or detecting technical faults might consititute a legitimate interest of the service provider.**

**Similarly, using the processing storage capabilities of terminal equipment is to fix security vulnerablities and other security bugs, provided that such updates do not in any way change the functionality of the hardware or software or the privacy settings chosen by the end-user and the end-user has the possibility to postpone or turn off the automatic installation of such updates. Software updates that do not exclusively have a security purpose, for example those intended to add new features to an application or improve its performance, should not be considered as a legitimate interest.**

**A legitimate interest could also be relied upon by a service provider whose website content or services are accessible without direct monetary payment and wholly or mainly financed by advertising, provided that these services safeguard the freedom of expression and information including for journalistic purposes, such as online newspaper or other press publications as defined in Article 2(4) of Directive (EU) 2019/790, or audiovisual media services as defined in Article 1(1)(a)(i) of Directive 2010/13/EU[1], or radio programmes as mentioned in Directive 2019/789/EU, and the end-user has been provided with clear, precise and user-friendly information about the purposes of the cookies or similar techniques used and has ~~*accepted*~~ *been given the right to object*.**

**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 or similar devices for additional purposes 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. 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**

[1] As amended by Directive (EU) 2018/1808

~~**Conversely, a provider should not be able to rely upon legitimate interests if the storage or processing of information in the end-user's terminal equipment or the information collected from it were to be used to determine the nature or characteristics on a*n specific* end-user or to build an individual profile *of for attribution to an* specific end-user. In such cases, the end-user's interests and fundamental rights and freedoms override the interest of the service provider, as such processing operations can seriously interfere with one's private life, for instance when used *for segmentation purposes,* to monitor *or segment* the behaviour of a specific end-user or to draw conclusions concerning his or her private life. A legitimate interest should not exist if the information stored or processed in, or collected from, an end-user's terminal equipment includes special categories of personal data, as referred to in Article 9 (1) of Regulation (EU) 2016/679.**~~

~~**Consent should not be necessary either when the purpose of using the processing storage capabilities of terminal equipment is to fix security vulnerablities and other security bugs, provided that such updates do not in any way change the functionality of the hardware or software or the privacy settings chosen by the end-user and the end-user has the possibility to postpone or turn off the automatic installation of such updates. Software updates that do not exclusively have a security purpose, for example those intended to add new features to an application or improve its performance, should not fall under this exception.**~~

***Justification***

Recital 21b rightly recognizes services which safeguard the freedom of expression and information, including for journalistic purpose. Press publications, audiovisual media services but also radio should be able to rely on a legitimate interest for the processing of data. In order to align Recital 21b with the introduction of legitimate interest as a basis for processing the user "has been given the right to object", in order to ensure consistency with the balance of interest test and the language used in Recital 21c.

We also propose wording which clarifies the possibility for service providers to make access to their content conditional to the acceptance of cookies, aligning the Recital with our proposal in Article 8.1b.

**(21c) Where a service provider invokes a legitimate interest, certain additional conditions should be met and safeguards should be respected, including an impact assessment and where appropriate the consultation of the supervisory authority by the service provider. In addition, the service provider may ~~*not*~~ share the information with third ~~parties other than its processors, only in accordance with Article 28 of Regulation (EU) 2016/679, *unless it has been previously anonymised*~~ *provided that appropriate technical and organisational measures such as pseudonymisation and encryption are applied~~. ~~*The service provider should, where necessary, implement appropriate security measures, such as encryption and pseudonymisation*~~ to ensure privacy of the end-users. Moreover, the end-user should be provided with information about these processing operations taking place and be given the right to object to such operations.**

***Justification***

The changes brought to Recital 21 c are to ensure coherence with our suggested changes for Article 8.1a.

**Alternative Proposal Recital 21 c**

**(21c) Where a service provider invokes a legitimate interest, certain additional conditions should be met and safeguards should be respected, including an impact assessment and where appropriate the consultation of the supervisory authority by the service provider. In addition, the service provider should ~~*not*~~ share the information with third parties other than its processors~~, *only*~~ in accordance with Article 28*, or where applicable Article 26,* of Regulation (EU) 2016/679, ~~*unless it has been previously anonymised*~~ *provided that appropriate technical and organisational measures such as pseudonymisation and encryption are applied~~. ~~*The service provider should, where necessary, implement appropriate security measures, such as encryption and pseudonymisation*~~ to ensure privacy of the end-users. Moreover, the end-user should be provided with information**

**about these processing operations taking place and be given the right to object to such operations.**

***Justification***

The changes brought to the alternative proposal for a Recital 21 c are to ensure coherence with our suggested alternative changes for Article 8.1a, while providing for a clear alignment with the provisions in the GDPR.

Yours sincerely,


**Ilias Konteas**
EMMA
Ilias.konteas@magazinemedia.eu

**Ilias Konteas**
ENPA
ilias.konteas@enpa.eu

**Angela Mills Wade**
EPC
Angela.Mills-Wade@epceurope.eu

**Matt Payton**
AER
matt.payton@aereurope.org

**Dr. Bernd Nauen**
AIG
nauen@zaw.de

**Mathilde Fiquet**
FEDMA
mfiquet@fedma.org

**Agata Nowacka**
AMC
agata@dotcoms.eu

**Conor Murray**
EGTA
conor.murray@egta.com

**Jana Břeská**
SPIR
jana.breska@spir.cz

**Amélien Delahaie**
Geste
amelien@geste.fr

**Townsend Feehan**
IAB Europe
feehan@iabeurope.eu