The New ePrivacy-Regulation: Overview on the Most Important Changes

by Dr. Frank Eickmeier and Prof. Dr. Christoph Bauer

Hamburg, 16th January 2017 A draft of a new ePrivacy regulation from the European Commission was leaked as early as December 2016. Now the final version of 10/01/2017 has been published as an official proposal from the EU Commission. The new Regulation should replace the ePrivacy Directive 2002/58/EC in the coming years and flanks the General Data Protection Regulation (GDPR), which comes into force on 25 May 2018. Unlike the old ePrivacy Directive, the planned ePrivacy Regulation applies directly in all Member States and takes priority over national legislation. To the extent that it has been discussed in the past whether the ePrivacy Directive was fully implemented in Germany, this question is now superfluous with the Regulation now proposed, because this does not require any implementation by German legislators.

IAB Europe harshly criticized the draft in a first statement:

“The Commission had the perfect opportunity to prove its interests in better and smarter rules by doing away with the outdated and unnecessary Cookie Law”,

says Townsend Feehan, Managing Director of IAB Europe.

“Finally the Commission recognizes the important role of advertising for the financing of free online content and at the same time proposes a law which will inflict clear damage on this business model, all without offering the users genuine advantages for the protection of their private sphere and their data. Whoever finds cookie banners annoying will be disappointed to know it will not be any better.”

Criticism also came from German businesses. The “Bundesverband Digitale Wirtschaft” (BVDW) [German Federal Association of Digital Business] warned of a “fundamental threat to today’s information society”.

It should therefore be demonstrated below where the threat to traditional business models of the online economy could lie.

1) Current situation

The use of third party cookies is currently permitted by the law applicable in Germany, even without the consent of the user concerned, provided that the user is granted a right to opt out. This is so, even though the applicable ePrivacy Directive expects otherwise:

“Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing.” (Article 5 (3) ePrivacy Directive 2002/58/EC in version of Directive 2009/136/EC)

As the German Federal Court of Justice decided in the “Payback Judgement” of 2008 (BGHZ 177, 253 – Payback), Section 15 (3) Telemediengesetz (TMG) [German Telemedia Law] makes it clear that it is enough to offer an opt-out solution for the user to opt-out in the case of the use of communication data.

The wording of Section 15 (3) TMG is as follows:

“The service supplier may create use profiles using pseudonyms for the purposes of advertising, market research or needs-based organization of telemedia if the user does not opt-out of this. The service supplier is to inform the user of his opt-out right within the framework of the information provided pursuant to Section 13 (1). This use profile may not be brought together with data about the person to whom the pseudonym applies.”

In a statement by the German Federal Ministry of Economics on the implementation of the ePrivacy Directive, it states that the rule, also known as the “Cookie Directive”, was sufficiently implemented by the provisions of the German telemedia law. If no personal information is contained in third party cookies, these are in any case to be qualified as pseudonyms within the meaning of Section 15 (3) TMG, meaning that their use was permitted, provided that the user was given the possibility to opt-out of the particular website.
Because other Member States, such as the United Kingdom, implemented the ePrivacy Directive in a significantly stronger way, and above all on the basis of the strict data protection requirements of Google regarding users of Google AdSense, in practice many German website operators and cookie users deviated from obtaining user consent by inserting a “cookie banner”.

2) Content of the planned ePrivacy Regulation

The ePrivacy Regulation, along with the General Data Protection Regulation applicable from the end of May 2018, should regulate the area of electronic communication and the handling of personal data in particular.

The provisions of interest for cookies are contained in Articles 8 and 9. Of particular interest are the Recitals 21 to 24 prefixed to the Regulation, which deal explicitly with the use of tracking cookies and third party cookies. The recitals of a regulation are however not themselves part of the legislative text. They do however reflect the thoughts and considerations of the EU Commission and aid interpretation of the wording of the legislation. The Recitals mentioned state as follows:

“(21) Exceptions to the obligation to obtain consent to make use of the processing and storage capabilities of terminal equipment or to access information stored in terminal equipment 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 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. Cookies can also be a legitimate and useful tool, for example, in measuring web traffic to a website. 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.
(22) The methods used for providing information and obtaining end-user’s consent should be as user-friendly as possible. Given the ubiquitous use of tracking cookies and other tracking techniques, end-users are increasingly requested to provide consent to store such tracking cookies in their terminal equipment. As a result, end-users are overloaded with requests to provide consent. The use of technical means to provide consent, for example, through transparent and user-friendly settings, may address this problem. Therefore, this Regulation should provide for the possibility to express consent by using the appropriate settings of a browser or other application. The choices made by end-users when establishing its general privacy settings of a browser or other application should be binding on, and enforceable against, any third parties. Web browsers are a type of software application that permits the retrieval and presentation of information on the internet. Other types of applications, such as the ones that permit calling and messaging or provide route guidance, have also the same capabilities. Web browsers mediate much of what occurs between the end-user and the website. From this perspective, they are in a privileged position to play an active role to help the end-user to control the flow of information to and from the terminal equipment. More particularly web browsers may be used as gatekeepers, thus helping end-users to prevent information from their terminal equipment (for example smart phone, tablet or computer) from being accessed or stored.

(23) The principles of data protection by design and by default were codified under Article 25 of Regulation (EU) 2016/679. Currently, the default settings for cookies are set in most current browsers to ‘accept all cookies’. Therefore providers of software enabling the retrieval and presentation of information on the internet should have an obligation to configure the software so that it offers the option to prevent third parties from storing information on the terminal equipment; this is often presented as ‘reject third party cookies’. End-users should be offered a set of privacy setting options, ranging from higher (for example, ‘never accept cookies’) to lower (for example, ‘always accept cookies’) and intermediate (for example, ‘reject third party cookies’ or ‘only accept first party cookies’). Such privacy settings should be presented in an easily visible and intelligible manner.

(24) For web browsers to be able to obtain end-users’ consent as defined under Regulation (EU) 2016/679, for example, to the storage of third party tracking
cookies, they should, among others, require a clear affirmative action from the end-user of terminal equipment to signify his or her freely given, specific informed, and unambiguous agreement to the storage and access of such cookies in and from the terminal equipment. Such action may be considered to be affirmative, for example, if end-users are required to actively select ‘accept third party cookies’ to confirm their agreement and are given the necessary information to make the choice. To this end, it is necessary to require providers of software enabling access to internet that, at the moment of installation, end-users are informed about the possibility to choose the privacy settings among the various options and ask them to make a choice. Information provided should not dissuade end-users from selecting higher privacy settings and should include relevant information about the risks associated to allowing third party cookies to be stored in the computer, including the compilation of long-term records of individuals' browsing histories and the use of such records to send targeted advertising. Web browsers are encouraged to provide easy ways for end-users to change the privacy settings at any time during use and to allow the user to make exceptions for or to whitelist certain websites or to specify for which websites (third) party cookies are always or never allowed.”

In Recitals 21 to 24, the EU Commission assesses the current position of data protection online. There are currently far too many requests made to users for consent. These many requests for consent expect too much of internet users (Recital 22). It is therefore necessary, on the one hand, to exclude data processing with low levels of relevance from the requirement to obtain consent. For example, no consent should be required if a session cookie is used which facilitates completing an online form with several pages. It should be possible to use this cookie without separate consent (Recital 21). The user should also not have to be asked separately about “technically required” tracking cookies, such as to measure a website’s traffic.

According to the regulation proposed by the Commission, however, the consent of the user concerned should be required for all remaining third party cookies and other tracking cookies. According to our initial assessment, this provision would have significant effects on the entire online industry.

On the form of the consent, the EU Commission in Recitals 21 - 25 prioritizes the concept that consent can in future be granted by way of the data protection settings in the browser of the user affected. This would be possible if the user is well aware when making the corresponding
setting in the browser that he is consenting to the placement of tracking cookies. With reference to the planned provisions on privacy by design in Regulation 2016/679/EU, the EU Commission invokes the browser producers to create more transparency and clarity regarding the settings on data protection. By simple and comprehensible means, the producers should give the user the option in the browser settings to decide between, for example, “accept no cookies”, “reject third party cookies” and “only accept first party cookies”. Already when installing the browser, the user should be informed about the possible data protection settings and asked to make a choice.

A first consent should be revocable according to Recitals 34 and 35, and indeed at any time, and it should be as simple as possible.

Apart from the use of cookies, Recital 20 has another particular relevance. According to it, the consent of the user will be required for the use of many techniques for processing the information on the consumer’s end device.

(20) […] “Given that such equipment contains or processes information that may reveal details of an individual’s emotional, political, social complexities, including the content of communications, pictures, the location of individuals by accessing the device’s GPS capabilities, contact lists, and other information already stored in the device, the information related to such equipment requires enhanced privacy protection. Furthermore, the so-called spyware, web bugs, hidden identifiers, tracking cookies and other similar unwanted tracking tools can enter end-user’s terminal equipment without their knowledge in order to gain access to information, to store hidden information and to trace the activities. Information related to the end-user’s device may also be collected remotely for the purpose of identification and tracking, using techniques such as the so-called ‘device fingerprinting’, often without the knowledge of the end-user, and may seriously intrude upon the privacy of these end-users. Techniques that surreptitiously monitor the actions of end-users, for example by tracking their activities online or the location of their terminal equipment, or subvert the operation of the end-users’ terminal equipment pose a serious threat to the privacy of end-users. Therefore, any such interference with the end-user’s terminal equipment should be allowed only with the end-user’s consent and for specific and transparent purposes.”
In contrast, the EU Commission, according to Recital 25, states that connection data, such as the MAC address or IMEI number of end devices, may be used without the consent of the user, provided there is not a high level of risk for the user’s data security. Insofar as such connection data will be collected, the users must be shown clear information already before the collection of data so that the user can evade the collection his data, like video-surveillance areas.

In Recital 32 of the Regulation, the term “direct marketing” is described as any kind of advertising which is sent to the end user via electronic communication. This also includes messages from political parties and non-profit organizations.

In Recital 17, the EU Commission sees the requirement on the use of metadata (“electronic communications metadata”) by the providers of communications services, such as for the improvement of public transport and infrastructure. For these purposes, it is not necessary to anonymize the data, but rather use of the metadata is permissible with an “identifier”. Insofar as high risks are involved in the processing of these metadata, a data protection impact assessment and prior consultation with the supervisory authorities must be undertaken by way of Articles 35 and 36 of the GDPR 2016/679/EU.

3) The provisions in detail

The Commission proceeds as follows from a technical legal standpoint: Pursuant to Art. 8 (1) of the proposed Regulation, the use of “processing and storage capacity” of the “user’s end device” is fundamentally forbidden, unless the user grants his consent or the use of processing and storage capacity is necessary for the presentation of the website and for measuring web traffic.

“Article 8 Protection of 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."

Art. 8 (1)(a) benefits website operators in particular, who now no longer need any separate consent from the user to use compulsory cookies, without which accessing the content of the website would not be possible. But other cookies, such as tracking and session cookies, are permitted without consent if they are required for the presentation of Information Society services and the user accesses them.

In doing so, the term "Information Society service", as formerly defined in Art. 1 (2) of Directive 98/34/EC in the version of Directive 98/48/EC, has a broad meaning.

"2. ‘Service’: an Information Society service, i.e. any service performed generally against payment electronically with distance selling and on individual access by a recipient.

This definition has the following meanings

- ‘service performed by distance selling’ is a service which is performed without the simultaneous physical presence of the contract parties;

- ‘services performed electronically' means a service which is sent to the gateway and received at the end point using devices for electronic processing (including digital compression) and storage of data, and which is sent, forwarded and received fully via wire, radio, optical or other electromagnetic routes;

- ‘service performed on individual access by a recipient' means a service which is performed through the transfer of data following individual request.”

Tracking cookies for web forms and session cookies for measuring web traffic are mentioned as examples in the Recitals.

Whether analysis tools like Google Analytics also fall under the exceptions of Art. 8 (1)(c) depends on the interpretation of the limitation “carried out by the provider”. This is problematic here because Google Analytics is not identical to the website operator, which offers the desired
Information Society service. In any case, Google Analytics is not a case under Art. 8 (1)(a) because the service is not required for the transfer of content.

Art. 8 (2) of the Regulation also addresses data which the user’s end device transmits when communicating in the network. This involves in particular the IP address and the user agent. Storing this data should fundamentally be prohibited, unless this is “required to establish a connection”.

By way of exception, these data may be gathered if a “clearly and obviously visible” notification is shown, which states how, from whom and for what reason the data will be stored, as well as explaining the steps which the user can take to “minimize” this data processing. This may also include the tracking and connection data, such as via the MAC address or the IMEI number. In this regard, at first sight it appears that Recitals 20 and 25 contradict one another. It is probably evaluative to observe how severely the tracking of the user invades his private sphere.

“Article 8 Protection of information related to end-users’ terminal equipment
[...] 2. The collection of data emitted by terminal equipment to enable it to connect to another device and or network equipment by natural or legal persons other than end-users concerned shall be prohibited, except:
(a) if it is done exclusively in order and for the time necessary to establish a possible connection;
(b) if a clear and prominent notice is displayed to the public informing of, at least, the modalities of the collection its purpose, the person responsible for it and of any measure the end-user of the terminal equipment can take to minimise the collection, and,
When such data is used for direct marketing and profiling, the end-user shall have the right to object as provided for in Article 21 of the GDPR [...]”

Art. 9 of the proposed Regulation governs the form of user’s consent, which takes priority according to Art. 7 of the coming General Data Protection Regulation. According to this, the consent is fundamentally possible without a particular form, but must be provably documented and can be revoked at any time.
Pursuant to Article 9 (2) of the proposed Regulation, the consent can also be granted by way of the user’s settings in the browser, but only “insofar as this is technically possible and effective”. Should the user configure the data protection settings in his browser according to this requirement in such a way that third party cookies are allowed, he consents to the placement of cookies when visiting a website:

“Article 9 Consent
1. The definition of and conditions for consent provided for under Articles 4(11) and 7 of Regulation (EU) 2016/679/EU shall apply.
2. Without prejudice to paragraph 1, where technically possible and feasible, for the purposes of point (b) of Article 8(1), consent may be expressed by using the appropriate technical settings of a software application enabling access to the internet.
3. End-users who have consented to the processing of electronic communications data as set out in point (c) of Article 6(2) and points (a) and (b) of Article 6(3) shall be given the possibility to withdraw their consent at any time as set forth under Article 7(3) of Regulation (EU) 2016/679 and be reminded of this possibility at periodic intervals of 6 months, as long as the processing continues.”

If one observes the Recitals explained above, the terms “technically possible and effective” must however mean that the browser used by the user allows the user to configure the data settings with sufficient transparency and simplicity, so that it corresponds with the user’s actual will if he agrees to the use of third party cookies or tracking cookies requiring consent. More precisely, it cannot be said at this point, because it is unclear, whether and how Art. 25 (1) of the coming General Data Protection Regulation 2016/670/EU (Privacy by Design) will be implemented with the obligation for producers to design products in a data-friendly way.

In this regard, the EU Commission determined in Article 10 of the Regulation that any software which opens up electronic communication, should offer an option to prevent the storage of information on the end device or the use of processing power of the end device by third parties. According to paragraphs 2 and 3, the producer should explain to the user the corresponding options on data protection already at the point of installation or by way of an update.

According to Article 9 (3) of the Regulation, any consent granted by the user must be revocable at any time. The user must be reminded about the option to revoke his consent in six-month intervals, but only if the data are still being processed. If a cookie is placed after consent is
granted, the user must be given the possibility at the end of six months to revoke the consent to the cookie. If he does so, the cookie must be deleted or de-activated.

Should the proposed Regulation therefore be implemented in this way, the legal position for cookies in the EU will be significantly more difficult. It does not correspond with what the EU Commission wanted at all, which was to cut the water from the online advertising industry dependent on cookies, because it wants to give the user himself the decision about how his user data is dealt with.

But to strengthen the user’s position, the proposed Regulation should also be directed against “surreptitious monitoring” of the user. Nevertheless, the use of processing and storage capacity of the end user device should be regulated more strongly, which is expected to have extensive consequences.

In fact, the planned Regulation should follow the approach of “Privacy by Design”. Software producers should adapt their products in such a way that the user receives more clarity about the use of their personal data and can control this better. It is not yet possible to assess how the large browser producers will react to this.

Insofar as it is not made clear how browser settings are to look in order to meet the EU Commission’s requirement of being “technically possible and effective”, the planned ePrivacy Regulation should also lead to a situation where both the placement of cookies as well as the processing of IP addresses and user agents Europe-wide is dependent on the prior consent of the user concerned. Solving the problem with an opt-out, a notification in the privacy policy or a simple notification banner would therefore be passé.

Finally, the ePrivacy Regulation, because it is coupled with the General Data Protection Regulation, will have a much more extensive effect, including for companies outside of the European Union, because the rights of visitors to websites from the EU must be observed at the same time.

4) Outlook

Unlike for the General Data Protection Regulation with its long transitional period, the ePrivacy Regulation should come into force six months after it is published (Art. 31 (2)). It is therefore important to keep a close eye on further legislative processes.
If there is a violation of the requirements presented, the responsible supervisory authority can impose draconian penalties of up to 20 million euros, or 4 % of the company’s income. Companies affected should therefore certainly prepare to implement the new rules.

5) Summary

According to the current proposal of the ePrivacy Regulation, only visiting a website by the end user can no longer be understood as consent to separate data processing.

The currently customary banner with the content “By visiting this website, you (by implication) accept the use of cookies” or the notification “We use cookies” and an OK button will become impermissible because the user does not really have a genuine choice regarding giving consent. It is also not enough to provide information that the user affected can set up data protection in his browser.

Rather, on first accessing the website and even before the first placement of a cookie requiring consent, the user must be notified about the use of cookies, at which point the user has the option to agree or to reject. The notification can be presented by way of a banner or a notification window which cannot be overlooked. The consent must be requested by way of an opt-in. Opt-in means that, if a checkbox is used, this may not already be filled in with a tick. The user must explicitly click on “Agree” himself in order to agree, as if he were concluding a purchase online. If he does not do this and does not pay attention to the banner/notification, no cookies which require consent may be placed.

Should the user refuse, the website may not however be blocked to him. In Recital 42 of the General Data Protection Regulation, it states that the design must be such that the user “[…] is in the position to refuse or revoke the consent without suffering disadvantages.” But there are plausible reasons to accept a disadvantage if the user who does not consent would be deprived of content in the website. But this cannot be said with absolute certainty because it is currently unclear how a “disadvantage” will be defined.

Besides that, the website operator must also offer users who have already granted their consent an opt-out at any time, that is to say an option to later revoke their consent.

Not least, website operators have to consider in future also the browser setting “Do Not Track” because this already establishes the non-consent of the user.
Strict compliance with the new rules of the ePrivacy Regulation will lead to significant expenses for the website operators to adapt the website. Especially in the case of website monitoring, companies must in future weigh up very precisely what forms of data collection require user consent. Intensive negotiations and a lot of lobbying work is expected before the norm comes into force.