Guidance Note:
Cookies and other tracking technologies

April 2020

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Contents

The DPC's regulatory role in relation to cookies and tracking technologies

The Data Protection Commission is the national authority responsible for the enforcement of the law on ePrivacy, that is to say the EU ePrivacy Directive (2002/58/EC as amended by 2009/136/EC), and the Irish ePrivacy Regulations, implemented by Statutory Instrument (S.I.) No. 336 of 2011. This legislation is separate to, but complements, the General Data Protection Regulation. Organisations must comply with both laws, but the rules under the ePrivacy legislation apply first when you are considering your organisation's use of cookies and other tracking technologies. Regulation 5 of the ePrivacy Regulations is the relevant legislation regulating the use of cookies.

The ePrivacy Regulations

Regulation 5 of the ePrivacy Regulations

Regulation 5 *of the European Communities (Electronic Communications Networks and Services)(Privacy and Electronic Communications) Regulations 2011 (S.I. No. 336 of 2011) ('the ePrivacy Regulations') protects the confidentiality of communications.*

Regulation 5(3): *A person shall not use an electronic communications network to store information, or to gain access to information already stored in the terminal equipment of a subscriber or user, unless*

(a) the subscriber or user has given his or her consent to that use, and

(b) the subscriber or user has been provided with clear and comprehensive

information in accordance with the Data Protection Acts which—

(i) is both prominently displayed and easily accessible, and

(ii) includes, without limitation, the purposes of the processing of the information.

Regulation 5(4): *For the purpose of paragraph (3), the methods of providing information and giving consent should be as user-friendly as possible. Where it is technically possible and effective, having regard to the relevant provisions of the Data Protection Acts, the user's consent to the storing of information or to gaining access to information already stored may be given by the use of appropriate browser settings or other technological application by means of which the user can be considered to have given his or her consent.*

Regulation 5(5): *Paragraph (3) does not prevent any technical storage of, or access to, information for the sole purpose of carrying out the transmission of a communication over*

an electronic communications network or which is strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.

Regulation 5(5) therefore sets out the criteria a cookie or other tracking technology must meet in order to be exempt from the requirement to obtain consent.

What are cookies?

Cookies are usually small text files stored on a device, such as a PC, a mobile device or any other device that can store information. Devices that may use cookies also include so-called 'Internet of Things' (IoT) devices that connect to the internet.

Cookies serve a number of important functions, including to remember a user and their previous interactions with a website. They can be used, for example, to keep track of items in an online shopping cart or to keep track of information when you input details into an online application form. Authentication cookies are also important to identify users when they log in to banking services and other online services.

Certain cookies are also used to help web pages to load faster and to route information over a network.

The information stored in cookies can include personal data, such as an IP address, a username, a unique identifier, or an email address. But it may also contain non-personal data such as language settings or information about the type of device a person is using to browse the site.

Advertising IDs, user IDs and other tracking IDs may also be contained in cookies.

Cookies may be either *first party* or *third party* cookies. In general, a cookie set by your own website, i.e. the host domain, is a first-party cookie. A third-party cookie is one set by a domain other than the one the user is visiting, i.e. a domain other than the one they can see in their address bar. Such cookies can be related to advertising or to social media plugins enabled by the controller of the website, such as in the form of a 'like' button or a sharing tool.

Cookies may also have an *expiry date*. Session cookies, for example, which are designed to only function for the duration of a browser session or slightly longer, are likely to have a very short lifespan or expiry date and to be set to expire once they have served their limited purpose. The expiry date of a cookie should be proportionate to its purpose. Therefore, a session cookie used for a function such as remembering information in a shopping cart, or a user's travel details for a single journey, should not have an indefinite expiry date and should be set to expire once it has served its function or shortly afterwards.

What other types of tracking technologies are in use?

The cookies most internet users are aware of are typically browser, or http, cookies. However, other types of cookies and tracking technologies include local storage objects (LSOs) or 'flash' cookies, software development kits (SDKs), pixel trackers (or pixel gifs), 'like' buttons and social sharing tools, and device fingerprinting technologies. The law on cookies generally applies to *all of these tools.*

Cookies and other tracking technologies, including pixels, location tracking and device fingerprinting generally require the consent of the user because they involve access to information, or the placing of information on, a user's device or terminal equipment. There are only two circumstances where cookies are exempt from the requirement to obtain consent and these are outlined in detail below.

What is terminal equipment?

Any device, such as a PC or laptop, a mobile phone, an internet-connected device on which information may be stored or even a toy or a voice-activated assistant which uses cookies or other tracking technologies can be considered "terminal equipment" for the purposes of the Regulations.

What is the law on cookies and what is its purpose?

The ePrivacy Directive, which is transposed into Irish law in the 2011 ePrivacy Regulations, protects the privacy of the communications of individuals.

The terminal equipment (i.e. computers and other devices, including mobile phones) of users of electronic communications networks and any information stored on such equipment are part of the private sphere of users, requiring protection under international human rights instruments.

Technologies that use spyware, web bugs, hidden identifiers and other similar devices can be used to access a person's device without their knowledge, possibly storing hidden information that is used to trace that person's activities, movements and their online and offline habits. Such access to their devices without their consent or knowledge may seriously intrude upon the privacy of these users.

The purpose of the law on cookies is to protect individuals from having information placed on their devices, or accessed on their devices, without their consent, that may interfere with the confidentiality of their communications.

The law applies to any storage of information on a user's device or equipment, as well as to access to any information already stored on the equipment – this means through the use of browser cookies or other technologies such as device fingerprinting or the use of pixels or similar devices. It is irrelevant whether the information stored or accessed consists of, or contains, personal data. The ePrivacy Regulations apply when any information[1] is stored on or accessed from the device.

Additionally, where cookies contain identifiers that may be used to target a specific individual, or where information is derived from cookies and other tracking technologies that may be used to target or profile individuals, this will constitute personal data and its processing is also subject to the rules set out in the General Data Protection Regulation (GDPR).

Recital 30 of the GDPR notes that individuals (i.e. "natural persons") may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags.

It notes that this may leave traces which, "in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them".[i]

Online identifiers are also included in the definition of personal data in Article 4(1) of the GDPR.

Consent

The ePrivacy Regulations require that you obtain consent in order to gain any access to information stored in the terminal equipment of a subscriber or user, or to store *any information* on the person's device. This means you must get consent to store or set cookies, regardless of whether the cookies or other tracking technologies you are using contain personal data.

Consent for the setting of cookies must be of the standard defined in the General Data Protection Regulation Article 4(11), which says the 'consent' of the data subject means any "*freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*".

[1] The *Planet49* judgment of the Court of Justice of the European Union of 1 October 2019 clarifies that Article 5(3) of the ePrivacy Directive in relation to the storage of information, or access to information stored, on a user's terminal equipment applies whether or not the information is personal data.

Which cookies are exempt from the requirement to obtain consent from the user or subscriber?

As a controller, you are potentially using cookies for analytics purposes or for marketing, targeting or profiling purposes and you may choose to assign them to certain categories when you provide information for users on your website. However, regardless of how you choose to categorise them, cookies that do not meet one of the two specific use cases in the ePrivacy Regulations that make them exempt from the need to obtain consent *must not be set* or deployed on a user's device before you obtain their consent.

The two exemptions are known as a) the communications exemption and b) the strictly necessary exemption.

a) The communications exemption

This applies to cookies whose ***sole purpose*** is for carrying out the transmission of a communication over a network, for example to identify the communication endpoints. This may also apply to cookies used to allow data items to be exchanged in their intended order, i.e. by numbering data packets. It also applies to cookies used to detect transmission errors or data loss.

The Article 29 Working Party is clear in its Opinion 4/2012 on the Cookie Consent Exemption that this criterion *specifically limits the types of processing* which may be undertaken using cookies and does not leave much room for interpretation. Simply using a cookie to assist, speed up or regulate the transmission of a communication over a network is not sufficient for it to benefit from the consent exemption.

EXAMPLE 1: If you use a load-balancing cookie to distribute network traffic across different servers, this can be considered a type of cookie that meets the communication exemption. The information in this cookie has the sole purpose of identifying one of the servers (i.e. the communication end point) and it is therefore necessary to carry out the communication over the network.

b) the *strictly necessary* exemption

A cookie that is exempt under this criterion must simultaneously pass two tests:

The exemption applies to 'information society services' (ISS) – i.e. a service delivered over the internet, such as a website or an app. In addition, that service must have been *explicitly requested* by the user and the use of the cookie must be restricted to what is strictly necessary to provide that service. Cookies related to advertising are not strictly necessary and must be consented to.

EXAMPLE 1: Your website uses session cookies to keep track of items a user places in an online shopping basket. These cookies expire at the end of their session or shortly afterwards. These cookies meet the 'strictly necessary' condition and they do not require consent. Similarly, cookies that record a user's language or country preference when they visit your site can be considered strictly necessary to deliver a service explicitly requested by the user and they do not need consent.

EXAMPLE 2: A travel website deploys a cookie with a two-year lifespan used to uniquely identify a user's browser and device for the purposes of displaying a journey planner and for remembering their journey preferences each time they visit. This cookie is set without consent when the user lands on the site. While such functionality may be helpful to some users, these cookies require consent.

It should be clear to the user how long this preference is retained by your website for the purposes of presenting a journey planner in a browser or app. If the user is merely buying a ticket and enters a start and end point for their journey, this purpose may be served by means of a session cookie. However, if you wish to provide a service that allows your website to remember a user's journey preferences for a longer period, the cookie that functions to save this preference requires consent.

EXAMPLE 3: Your website has a chatbot function to allow people engage with customer service agents via an online chat window. Any cookies used to deliver that chat functionality must not be deployed until the person *explicitly requests* to use the chatbot. Such cookies do not meet the 'strictly necessary' consent exemption.

Opinion 04/2012 of the Article 29 Data Protection Working Party provides more detailed information to help you to assess which cookies may avail of one of the consent exemptions.

Opinion 9/2014 of the Article 29 Data Protection Working Party also clarifies that Article 5(3) of the ePrivacy Directive (as implemented in Irish law in Regulation 5(3)) applies to device fingerprinting technologies. This means that if you process device fingerprints which are generated through the storage of information, or the gaining of access to information, on a user's device that you may only do so with the valid consent of the user.

Do analytics cookies require consent?

Yes. Analytics cookies are used as a measuring tool for websites, including to provide information on the number of unique visitors and the pages they browse during their visits. Some analytics may use first-party cookies with the analytics function carried out by the controller or by another party on behalf of the controller. The Article 29 Working Party has clarified that this other party will be a joint controller or a processor,

depending on whether it uses the data for its own purposes or whether it is prohibited from doing so by contractual arrangements.

Third-party analytics carried out by parties other than the controller, sometimes for their own purposes, may be considered to represent a greater privacy risk to the user.

The Article 29 Working Party considers that first-party analytics cookies are not likely to create a privacy risk when they are strictly limited to first-party aggregated statistical purposes, and when they are used by websites that already provide clear information about such cookies in their privacy policy, as well as adequate privacy safeguards. This should include a user-friendly mechanism to opt out of any data collection for analytics.

It is unlikely that first-party analytics cookies would be considered a priority for enforcement action by the DPC.

Can you obtain consent for multiple purposes at the same time?

Consent may not be "bundled" for multiple purposes. As a matter of good practice, you should outline in a first layer of communication on your site or mobile app that you are requesting consent for the use of cookies for specific purposes. A second layer of information may then be used to provide more detailed information about the types of cookies or other technologies in use, with options for the user to opt in or to accept these cookies. You are not permitted to use pre-checked boxes, sliders or other tools set to 'ON' by default to signal a user's consent to the setting or use of cookies.

Withdrawal of consent

The user must be able to withdraw consent *as easily as they gave it* and you must not 'bundle' consent for cookies with consent for other purposes, or with terms and conditions for a contract for other services you provide. You should provide information in your cookies information about how users can signify and later withdraw their consent to the use of cookies, including by providing information on the action required for them to signal such a preference.

If you use a cookie to store a record that a user has given consent to the use of cookies, you should ask the user to reaffirm their consent no longer than six months[2] after you have stored this consent state. As a practical solution, consider the use of an easy tool,

[2] While the legislation does not prescribe a specific lifespan for such cookies, based on a first-principles analysis by the DPC, we consider this to be the appropriate default outer timeframe for storing the user's consent state. A controller would need to objectively and on a case-by-case basis justify storage for a longer period.

such as a 'radio button' on your website which allows users to control which cookies are set and to allow them vary their consent at any time.

Any record of consent must also be backed up by demonstrable organisational and technical measures that ensure a data subject's expression of consent (or withdrawal) can be effectively acted on.

How do you obtain consent in practice?

Most websites choose to implement a cookie banner or pop-up, which displays when a user lands on the website and which provides the first layer of information about the use of cookies and other tracking technologies. This banner or notice will also often contain a link to a cookies policy and a privacy policy which provide further, more detailed information.

If you use a cookie banner or pop-up, you must not use an interface that 'nudges' a user into accepting cookies over rejecting them. Therefore, if you use a button on the banner with an 'accept' option, you must give equal prominence to an option which allows the user to 'reject' cookies, or to one which allows them to manage cookies and brings them to another layer of information in order to allow them do that, by cookie type and purpose.

The user's consent must be specific to each purpose for which you are processing their data, it must be freely given and unambiguous and it requires a clear, affirmative action on the part of the user. Silence or inaction by the user cannot constitute their consent to any processing of their data.

You must include a link or a means of accessing further information about your use of cookies and the third parties to whom data will be transferred when the user is prompted to accept the use of cookies.

Can you use implied consent for the use of cookies and tracking technologies?

You may not obtain consent by 'implication' to set cookies. This means that wording in your cookie banner or notice which inform users that, by their continued use of your website – either through clicking, using or scrolling it - that you will assume their consent to set cookies, is not permissible.

Similarly, cookie banners that pop up when a user lands on a website and which subsequently disappear when a user scrolls, without any further engagement by the

user with the banner or with information about cookies, are not compliant with the law. You cannot assume that a user who merely scrolls a page or clicks an element on the page has seen and read the information in a cookie banner, unless you can demonstrate clearly that they have engaged with the information and given their unambiguous consent to the setting of cookies and the purposes of the processing.

Clear and comprehensive information

Regulation 5(3) of the ePrivacy Regulations requires that the user must be provided with "clear and comprehensive information" about the use of cookies in accordance with data protection law. While "clear and comprehensive" is not defined in the Regulations, the standard required must be in accordance with data protection legislation, i.e. the GDPR and the Data Protection Act 2018. In practice, if your processing involves personal data, you will need to meet the transparency requirements under Articles 12-14 of the General Data Protection Regulation. This means that there may sometimes be duplication in the information provided in your cookies policy and your privacy policy. It is still good practice to maintain both, in order to facilitate the different layers of information that may be required under the ePrivacy Regulations and the GDPR.

Transparency information and responsibilities under the GDPR

Where your processing, at the point after the cookies have been set, involves personal data, the GDPR applies to this processing. This means you must provide individuals with all the information to which they are entitled under Articles 12-13 of the GDPR in relation to transparency, including information about what other parties are processing their personal data. You must also provide information on how individuals may exercise all their data subject rights under the provisions of Chapter 3 of the GDPR, including how to make a subject access request and their right to make a complaint to a data protection authority.

Pre-checked boxes and sliders

These do not comply with European law, as has been clarified in the *Planet49* judgment of October 2019. Consent does not need to be given for each cookie, but it must be given for each purpose for which cookies are used. Where a cookie is used for more than one purpose that requires consent, such consent must be obtained for *all of those purposes* separately. Regardless of the description you choose to give a cookie (i.e. 'functionality', 'performance', 'analytics' or 'marketing'), the cookie must meet one of the

two exemption criteria in Regulation 5(5) in order to be exempt from the requirement to obtain a user's consent.

It does not matter whether cookies contain personal data. If they do not meet one of the criteria for the consent exemption, then you need to obtain the user's consent before you set them.

Requirements for the use of consent management providers (CMPs)

A consent management platform, or consent management provider (CMP) is a system used by some controllers to assist them in managing users' choices in relation to cookies and to help them meet their transparency obligations under data protection law. These are sometimes deployed in the form of software provided by a third-party vendor, or the controller may develop their own in-house platform to manage user consent and the provision of information about cookies and privacy choices. When a user visits a website and is presented with banners, pop-ups or sliders to manage their cookie consents, these choices are often being managed using a consent management platform of some form.

If you use a third-party CMP, the tool or software must do what it purports to do. It must not contain pre-checked boxes signalling 'consent' for the use of cookies. If such a third-party tool is used to keep a record of a user's consent to the use of cookies, you must also keep a record of that consent as part of your record of processing activities in accordance with Article 30 of the GDPR. You should limit the length of time such consent is valid for no longer than six months[3], after which time the user must be prompted to give their consent again.

Users must be able to withdraw or vary their consent for the use of cookies or tracking technologies at any time and you must make it clear how they may do this using the tools you have provided to manage consent. It must be as easy for a user to withdraw their consent as to give it.

[3] The legislation does not prescribe the period of time for which consent may be stored before a user is asked to reconfirm their choices. However, based on a first-principles analysis, we consider six months to be the appropriate outer time limit for such consent to be retained. Beyond that period, a controller would need to objectively justify its use of cookies with a longer lifespan to record a user's consent state.

Requirements for cookie banners

If you use a cookie banner to provide further information to users about your use of cookies, the banner must not obscure the text of your privacy policy or cookie policy. Users must always be able to read your cookies and privacy policies without any cookies (other than those falling into one of the two exemptions) being set. A banner that contains a link to more information about the use of cookies must link to easily readable text that is undisrupted by chatbots or other features on the page.

A banner that merely gives the user the option to click 'accept' to say yes to cookies and which provides no other option is not compliant. This means banners with buttons that read 'ok, got it!' or 'I understand', and which do not provide any option to reject cookies or to click for further, more detailed information, are not acceptable and they do not meet the standard of consent required.

You must at least provide information that allows the user to reject non-necessary cookies or to request more information about the use of cookies. In the second layer of information, you must provide further information about the types and purposes of the cookies being set and the third parties who will process information collected when those cookies are deployed.

Regardless of the means you choose to manage user consent, your user interface must meet the requirement that the information provided be clear and comprehensive.

Can you rely on the user's browser settings to infer consent?

In general, no. Users of your website or app cannot be deemed to have consented simply because they are using a browser or other application which by default enables the collection and processing of their information. As clarified by the Article 29 Working Party in its Opinion 2/2010 on Online Behavioural Advertising, average data subjects are not aware of the tracking of their online behaviour or the purposes of the tracking. They are not always aware of how to use browser settings to reject cookies, even if this information is included in privacy policies.

Even if you provide information in general terms and conditions and/or a privacy policy about third-party cookies used for behavioural advertising, including the basic uses/purposes of such cookies and how they can be avoided by setting the browser, this will not meet the "clear and comprehensive" information requirements of Regulation 5(3).

The circumstances where browser settings are likely to be considered valid to constitute consent to the setting of cookies are likely to be very limited and they would need to be assessed on a case-by-case basis.

Confusing interfaces

Take accessibility into account in designing your interfaces. If you use colour schemes for your cookie banners or your sliders and checkboxes that blend into the overall background of your site, these settings can be hard to navigate, particularly for people with vision impairments or colour blindness. While binary, colour-coded sliders or buttons may purport to signify a YES and NO option or an ON and OFF option, these colour schemes are not always accessible or self-explanatory to users who do not see colours the same way as other people. Consider testing your interface with users who have vision or reading impairments to make them as accessible as possible to all users.

Cookie lifespans

The lifespan of a cookie must be proportionate to its function. It would not be considered proportionate to have a session cookie with a lifespan of 'forever', for example.

Joint controllers

You should assess your relationship with the third parties whose assets you deploy on your website. This means that where you deploy 'like' buttons, plugins or widgets, pixel trackers or social media-sharing tools, you should be aware of what data you are sending to those third parties and of the fact that you may be considered a controller in respect of any personal data you collect and disclose to those third parties. This position was clarified by the Court of Justice of the European Union in the *Fashion ID* judgment of July 2019.

Consider also the relationship that might apply in a case where your website uses a third-party payment company to process payments for goods or services sold on your site. Aside from your responsibilities with regard to obtaining consent for cookies, if you use a third party to process payments, you will need a controller-processor contract in place with that organisation that meets the requirements of Article 28(3) of the GDPR. If that third party has any role in determining the means or the purposes of the processing of personal data passed to it by your organisation via cookies or other

means, it may also have a controller relationship in respect of that personal data. It is important that you consider the controller and processor responsibilities and liabilities arising from any relationships with third parties whose cookies are set via your domain.

Processing of personal data

It is not necessary that a cookie contain personal data in order that the user's consent be required to set it. However, where the use of cookies or the information derived from cookies involves the processing of personal data, this processing is subject to the rules of the General Data Protection Regulation and the Data Protection Act 2018.

This means you must also keep a record of the types of processing carried out that involve personal data. In practice, you should maintain a comprehensive record of each specific type of processing as part of your record of processing activities, which is required under Article 30 of the GDPR.

If you are processing personal data obtained from cookies or other tracking technologies and it is appended or linked to other data about an identifiable customer with an account or a loyalty card, for example, you must inform users and customers about this processing when they use your website or app, including how they may exercise their data subject rights under the GDPR.

If, as a result of using cookies, the information you process or collect can also be considered personal data, then you must comply with the rules of the GDPR as well as with the ePrivacy rules. Personal data includes online identifiers or numbers, such as those that may be contained in cookies and that relate to an identified, or identifiable, natural person. It does not matter whether your organisation is in possession of other information that may be needed to identify an individual; the fact that the person may be identified, even with the addition of information held by another organisation, is sufficient to make this data personal data.

Do you need to conduct a data protection impact assessment (DPIA)?

The DPC has published a list of processing operations for which a data protection impact assessment is mandatory. This includes processing operations involving the systematic monitoring, tracking or observing of individuals' location or behaviour, and the profiling of individuals on a large scale.

It also includes processing involving the combination, linking or cross-referencing of separate datasets where such linking significantly contributes to or is used for profiling or behavioural analysis of individuals. This is particularly the case where the data sets are combined from different sources and where processing was/is carried out for different purposes or by different controllers.

If your processing involves any of these operations, on foot of your use of cookies or otherwise, you must carry out a DPIA.

Special category data

If your organisation is processing special categories of personal data, including through information derived from cookies, this is subject to strict rules under the GDPR. Article 9 of the GDPR defines special category data as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. In general there is a prohibition on processing such personal data unless very specific exemptions apply. In practice, the only likely legal basis your organisation will have for processing any special category data derived from the use of cookies or other tracking technologies, is the **explicit** consent of those individuals whose data you are processing.

The bar to demonstrate that you have the explicit consent of users for the processing of their special category data is a high one and it is unlikely to be met by means of generic information in a cookie banner or privacy policy.

The processing of special category data must also comply with the principles relating to the processing of personal data in Article 5 of the GDPR and it must have a lawful basis, as required by Article 6 of the GDPR as well as meeting the requirements of Article 9.

Location tracking or derivation of location information from cookies

You must not use cookies or other technologies to track the location of a user or a device without consent. While location data is not listed as special category data in Article 9 of the GDPR, the Court of Justice of the European Union has recognised its particular sensitivity because it can be used to derive very precise information about individuals and their behaviour, including their everyday habits, their permanent or temporary places of residence, their daily movements and activities, their social relationships and the social environments they frequent[4]. If you set cookies that are used to track the location of a device or a user, you may only do this with the user's consent.

Compliance

The legal regime that currently must be complied with in Ireland is the ePrivacy Directive 2002 (as amended) and the ePrivacy Regulations (S.I. No. 336/2011). Controllers must not implement any unlawful changes to their cookies policies or their deployment of cookies and other tracking technologies based on their interpretation of proposals for legislation that is not agreed and that has not been enacted. The DPC will allow a period of six months from the publication of this guidance for controllers to bring their products, including websites and mobile apps, into compliance, after which enforcement action will commence."

6 April 2020

[i] General Data Protection Regulation (EU) 2016/679 of the European Parliament and the Council (Recital 30).

[4] Tele2 Sverige AB (C-203/15) judgment of 21 December 2016: http://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=3318435