DMI's processing of personal data about website visitors

Date: 11-02-2020

Decision

Public authorities

On the basis of a complaint, the Danish Data Protection Agency has expressed serious criticism of DMI's processing of personal data in connection with the display of banner advertisements on the department's website.

Journal number: 2018-32-0357

The Danish Data Protection Agency hereby returns to the case, where [complainants] on 29 August 2018 complained to the Danish Data Protection Agency about the Danish Meteorological Institute's (hereinafter DMI) processing of personal data about him in connection with displaying banner ads on DMI's website (www.dmi.dk).

The case has been discussed at a meeting of the Data Council.

The Danish Data Protection Agency initially notes that since the submission of the complaint, DMI has concluded that personal data has been collected and passed on, including complaints, without a legal basis for processing, which is why the institute has changed the way in which consent is obtained for the collection and transfer of personal data. the visitors to dmi.dk.

With this decision, the Danish Data Protection Agency decides whether processing of personal data on complaints until DMI's change of the institute's procedure for obtaining consent has been justified, and whether the institute's current processing of personal data about visitors to dmi.dk takes place within the framework of the Data Protection Ordinance.

Decision

The Danish Data Protection Agency finds that neither DMI's previous nor current solution for obtaining consent for the processing of personal data about visitors to dmi.dk meets the Data Protection Ordinance's [1] requirements for the data subject's consent in Article 4, no. 11, and the basic principle of legality. fairness and transparency of Article 5 (1) 1, letter a.

Furthermore, the Danish Data Protection Agency finds that DMI's processing of personal data on complaints when collecting and passing on to Google has been - and is - in breach of Article 6 of the Data Protection Regulation, as none of the provisions of Article 6 (1) 1, the conditions mentioned have made / apply.

On the basis of the above, the Danish Data Protection Agency finds that there are grounds for expressing serious criticism that DMI’s processing of personal data about the visitors to dmi.dk, including complaints, has not taken place in accordance with

the Data Protection Ordinance.

2. Case presentation

It appears from the case that DMI shows banner ads on the department's website, including from e.g. Google's advertising platform whereby DMI contributes to the collection and transmission of personal information about the website's visitors to Google.

DMI has had banner ads on dmi.dk since 2004, and the income from this forms part of the department's funding basis.

2.1. Complainant's remarks

Complainants have generally stated that DMI displays banner ads on its website, including i.a. ads from the Google Ad Exchange advertising exchange, which uses personal information to personalize ads, e.g. information about visits to other websites.

Complainants have further stated that Google offers a number of services aimed at website owners who wish to buy and sell ads, both with and without Google as an intermediary. The services are marketed under the names DoubleClick, Google Ads, AdSense, AdWords and more. (hereafter Google's advertising platform). The Services are closely integrated and subject to the same guidelines for use, and for the majority of these services, Google is the data controller.

Ad joint data responsibility

Complainants have stated that DMI should be held jointly and severally responsible with Google for the collection and disclosure of personal information about him.

Furthermore, complainants have stated that Google is only able to collect personal information about him during his visit to dmi.dk and use it for targeting ads, because DMI has engaged Google to sell ads on dmi.dk and implemented Google's plugin (so-called ad tags) on dmi.dk.

Complainants have further stated that DMI by inserting these ad tags has the opportunity to specify a number of parameters that determine how the ads are selected and presented on dmi.dk, and that DMI thereby greatly contributes to determining for what purpose and by what means Google may process personal data. If DMI had not inserted these tags, Google would not be able to show ads to visitors to dmi.dk or track their behavior.

Complainants have further stated that DMI probably does not have access to the personal information that Google collects and processes about the visitors to dmi.dk, other than possibly in anonymised or aggregated form, but that this does not exclude

that there may be joint data responsibility. .

By consent

Complainants have stated that DMI has not obtained his consent to this processing and that DMI thus, in his view, has no legal basis for the processing of personal data about him.

Complainants have further pointed out that it is Google's own assessment that the processing of personal data that takes place in connection with Google's advertising platform cannot take place without the consent of the data subjects, ie. consent of the visitors to the websites that have implemented the advertising platform. Google therefore requires in its guidelines that the consent of visitors be obtained when an organization uses the advertising platform to display personalized banner ads.

In addition, the complainant is of the opinion that DMI, with the new solution for obtaining the consent of visitors, still does not meet the requirements of the Data Protection Regulation.

Furthermore, the complainants have stated that the consent has not been informed, as it is not clear to which third parties, including Google, personal information is passed on.

Complainants have further stated that in the consent solution use is made of pre-ticked fields, which cannot constitute a valid consent, and that the fields are even hidden, unless you select "Show details".

Finally, complainants have stated that it is only possible to obtain the necessary information by reading DMI's privacy policy, which, however, cannot be accessed before giving or refusing to give consent to the processing of personal data, and that any consent can therefore not is said to be informed.

Ad legitimate interest

Complainants have stated that DMI's legitimate interest in the processing of personal data about him does not take precedence over his rights and freedoms. In this connection, the complainants have pointed out that Google's advertising platform is widely used across the Internet, and that the collection and transfer of personal data to Google allows the company to draw a detailed picture of the complainants' movements across the Internet, which constitutes a significant encroachment on his rights and freedoms.

Finally, complainants have pointed out that it is possible for DMI to display banner advertisements which are not personalized in relation to the visitors on the basis of the processing of personal data about them.

2.2. DMI's comments

DMI has generally stated that the department processes information about complaints if he has given consent to the use of cookies on dmi.dk.

Ad joint data responsibility

DMI has acknowledged that the department, by integrating advertisements from e.g. Google's advertising platform on dmi.dk has contributed to the collection and disclosure of personal information about the website's visitors, including complaints.

By consent

DMI has acknowledged that the collection and transfer of personal information in question has taken place on an unauthorized basis with regard to complaints and other visitors who have opted out of the use of cookies on the website.

Furthermore, DMI has stated that this was an unintentional error, and that the department will therefore in the form of a news or pop-up window inform the visitors to dmi.dk that for a period cookies have been placed before and regardless , that consent had been given for this, as well as instructions on how to delete these cookies from the visitors' browser.

In addition, DMI has generally stated that the department has, after the complaint was submitted to the Danish Data Protection Agency, launched a new website where visitors are presented with a very clear consent solution. In order to proceed to the content of the website, it is necessary that the visitors take an active position on whether they will allow the use of cookies. If the visitors want to give consent, the consent is obtained by the visitors selecting "OK". If the visitors want to deselect cookies, select "Show Details", after which the visitors are given the opportunity to deselect cookies.

In this connection, DMI has sent a copy of the implemented consent solution, of which i.a. appears:

”DMI and third parties use cookies to make dmi.dk more usable, give you a better experience and for targeted marketing. By clicking OK here you give your consent to this. You can always withdraw your consent. Read more in our privacy policy. ”

In this connection, DMI has stated that it is possible to give consent to some cookies, while other cookies, e.g. marketing cookies, can be deselected.

DMI has stated that the source code for dmi.dk has been changed and that personal information will not be collected and passed on until the visitors have actively given their consent. Furthermore, DMI has stated that the consent solution has been changed so that the different types of cookies are no longer automatically pre-checked if you seek further information about these.

Finally, DMI has stated that in the future the department will make it clear to visitors that dmi.dk uses Google's advertising

platform. Visitors have been able to find cookies from Google in the list of selection cookies, but these are most often referred to by names that are not directly related to Google. Therefore, DMI will update its cookie and privacy policy on dmi.dk, so that it is clear that by accepting cookies, information is allowed to be passed on to Google, just as links will be added to Google's descriptions of how they use the personal information collected.

2.3. Google documentation

For the purpose of processing the case, the Danish Data Protection Agency has obtained publicly available information about Google's advertising platform.

Google's documentation [2] states, among other things. the following about the collection of information using Google's services:

"How Google uses information from sites or apps that use our services

Many websites and apps use Google services to improve their content and keep it free. When they integrate our services, these sites and apps share information with Google.

For example, when you visit a website that uses advertising services such as AdSense, including analytics tools such as Google Analytics, or embeds video content from YouTube, your web browser automatically sends certain information to Google. This includes the URL of the page that you're visiting and your IP address. We may also set cookies on your browser or read cookies that are already there. Apps that use Google advertising services also share information with Google, such as the name of the app and a unique identifier for advertising.

Google uses the information shared by sites and apps to deliver our services, maintain and improve them, develop new services, measure the effectiveness of advertising, protect against fraud and abuse and personalize content and ads that you see on Google and on our partners' sites and apps. "

Especially about advertising [3] appears i.a. following:

How Google uses cookies in advertising

Cookies help to make advertising more effective. Without cookies, it's harder for an advertiser to reach its audience, or to know how many ads were shown and how many clicks they received.

Many websites, such as news sites and blogs, partner with Google to show ads to their visitors. Working with our partners, we may use cookies for a number of purposes, such as to stop you from seeing the same ad over and over again, to detect and

stop click fraud and to show ads that are likely to be more relevant (such as ads based on websites that you have visited).

We store a record of the ads that we serve in our logs. These server logs typically include your web request, IP address, browser type, browser language, the date and time of your request, and one or more cookies that may uniquely identify your browser. We store this data for a number of reasons, the most important of which are to improve our services and to maintain the security of our systems. We anonymize this log data by removing part of the IP address (after 9 months) and cookie information (after 18 months).

Our advertising cookies

To help our partners manage their advertising and websites, we offer many products, including AdSense, AdWords, Google Analytics and a range of DoubleClick-branded services. When you visit a page or see an ad that uses one of these products, either on Google services or on other sites and apps, various cookies may be sent to your browser.

These may be set from a few different domains, including google.com, doubleclick.net, googlesyndication.com, googleadservices.com or the domain of our partners' sites. Some of our advertising products enable our partners to use other services in conjunction with ours (like an ad measurement and reporting service), and these services may send their own cookies to your browser. These cookies will be set from their domains. ”

About server logs, Google states the following [4]:

Like most websites, our servers automatically record the page requests made when you visit our sites. These "server logs" typically include your web request, Internet Protocol address, browser type, browser language, the date and time of your request, and one or more cookies that may uniquely identify your browser.

A typical log entry for a search for 'cars' looks like this:

123.45.67.89 - 25 / Mar / 2003 10:15:32 - http://www.google.com/search?q=cars - Firefox 1.0.7; Windows NT 5.1 - 740674ce2123e969

123.45.67.89 is the Internet Protocol address assigned to the user by the user's ISP. Depending on the user’s service, a different address may be assigned to the user by their service provider each time they connect to the Internet.

25 / Mar / 2003 10:15:32 is the date and time of the query.

http://www.google.com/search?q=cars is the requested URL, including the search query.

Firefox 1.0.7; Windows NT 5.1 is the browser and operating system being used.

740674ce2123a969 is the unique cookie ID assigned to this particular computer the first time it visited Google. (Cookies can be deleted by users. If the user has deleted the cookie from the computer since the last time they've visited Google, then it will be the unique cookie ID assigned to their device the next time they visit Google from that particular device). ”

3. The competence of the Data Inspectorate

Executive Order no. 1148 of 9 December 2011 on requirements for information and consent when storing or accessing information in the end user's terminal equipment (the cookie executive order), which has been issued pursuant to section 9 and section 81, subsection 1 of the Telecommunications Act. 2, regulates the extent to which information already stored in users' terminal equipment can be stored or accessed. This applies regardless of whether the information constitutes personal data or not.

The Cookie Executive Order contains rules that implement parts of Directive 2002/58 / EC of the European Parliament and of the Council (the e-Data Protection Directive), and it is the Danish Business Authority that supervises compliance with the Cookie Executive Order.

Of the cookie executive order § 3, para. 1, the following appears:

“Natural or legal persons shall not store information or access information already stored in an end - user's terminal equipment or allow third parties to store information or access information if the end user does not consent to it after receiving adequate information about the storage of or access to the information. "

Pursuant to the Data Protection Act, section 27, subsection 1, the Danish Data Protection Agency supervises compliance with the general data protection rules contained in the Data Protection Ordinance, the Data Protection Act and other legislation that falls within the framework of the Data Protection Ordinance for special rules on the processing of personal data.

In this connection, the Danish Data Protection Agency is of the opinion that rules implementing the e-Data Protection Directive do not constitute "other legislation that falls within the framework of the Data Protection Regulation for special rules on the processing of personal data", but rules implementing a parallel EU act. These are special rules that replace similar general rules in the Data Protection Regulation, whereas other legislation, such as certain provisions of the Health Act, constitute supplementary legislation to the Data Protection Regulation.

The supervision of rules on the processing of personal data, which has not been replaced by special rules implementing the e-Data Protection Directive, thus lies with the Danish Data Protection Agency.

Legal basis

4.1. The concept of personal data

The concept of personal data is defined in Article 4 (1) of the Data Protection Regulation as any information relating to an identified or identifiable natural person ('the data subject'). Identifiable natural person means a natural person who, on the basis of the information, can be directly or indirectly identified.

The opinion of the Article 29 Working Party on the concept of personal data [5] states in this regard:

"A" purpose element "may also be responsible for the fact that it is information" about "a particular person. The "purpose element" can be considered to exist when the information is used or - taking into account all the circumstances of the case in question - can be expected to be used for the purpose of assessing a person, treating the person in a certain way or influencing the person's status or behavior."

This view is reiterated by the Article 29 Working Party in its opinion on Behavioral Advertising on the Internet [6]. the following appears:

“Behavioral advertising usually involves the collection of IP addresses and the processing of unique identifiers (via the cookie). The use of such devices with a unique identifier makes it possible to track the users of a particular computer, even if dynamic IP addresses are used.

In other words, such devices make it possible to "designate" data subjects, even if their real names are not known. ii) The information collected in connection with behavioral advertising relates to (ie is about) a person's characteristics or behavior and is used to influence that particular person. This position is further confirmed if the possibility that profiles can be linked at any time to directly personally identifiable information provided by the data subject, e.g. registration-related information is taken into account. Other scenarios that can lead to identifiability are data merging, data loss and the increased availability of personal information on the Internet in combination with IP addresses. ”

Corresponding recital 30 in the preamble to the Data Protection Regulation states the following:

“Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as IP addresses and cookie identifiers, or other identifiers, such as radio frequency identifiers. This can leave traces that, especially when combined with unique identifiers and other information that the servers receive, can be used to create profiles of natural persons and identify them. ”

4.2. Data responsibility

Article 4 (8) of the Data Protection Regulation defines the data controller as a natural or legal person, a public authority, an institution or another body which, alone or together with others, decides for what purposes and with what aids processing may take place; of personal data.

Article 26 of the Data Protection Regulation on joint data controllers provides: 1:

“If two or more data controllers jointly determine the purposes and aids for processing, they are joint data controllers. They shall establish in a transparent manner their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercise of the data subject's rights and their respective obligations to provide the information referred to in Articles 13 and 14, by means of a arrangement between them, unless and to the extent that the respective responsibilities of the data controllers are laid down in EU law or the national law of the Member States to which the data controllers are subject. A contact point for registrants can be designated in the scheme. ”

In Case C-210/16 Wrtschaftsakademie Schleswig-Holstein, the European Court of Justice has ruled on joint data liability:

35 Although the mere fact of using a social network such as Facebook does not make a Facebook user co-responsible for the processing of personal data by this network, it should be noted that the administrator of a fan page on Facebook by creating such a page allows Facebook to to place cookies on the user's computer or any other medium when visiting the fan page, regardless of whether that person has a Facebook account.

36 In that context, it is apparent from the information provided to the Court that the creation of a fan page on Facebook implies that the administrator makes a recommendation which depends on, inter alia: the target group as well as the objectives for the management and advertising of its activities, which have an impact on the processing of personal data for the purpose of compiling statistics on the basis of the visits to the fan site. This administrator can, using the filters provided by Facebook, define the criteria on the basis of which the statistics are to be compiled and specify the categories of persons for whom Facebook is to collect personal data. Consequently, the administrator of a fan page on Facebook contributes to the processing of personal data about the users of his page.

37 The administrator of a fan page may in particular request to receive - and thus that demographic information about the target group, e.g. trends in age, gender, relationship status and employment, information on the lifestyle and areas of interest of the target group and information on the users of the site's purchases and buying behavior online, categories of goods or

services that interest the target group most, and geographical information that allows the fan site administrator to make specific sales promotions or arrange events or more generally to better target its information offerings.

38 While it is true that the statistics compiled by Facebook are only passed on to the fan page administrator in anonymised form, the compilation of these statistics is nonetheless based on the prior collection of users' personal information using cookies installed by Facebook in users' computer or any other medium when visiting the fan page and the processing of their personal data for statistical purposes. In any case, where several operators have joint responsibility for the same processing, Directive 95/46 does not require each individual to have access to the personal data in question.

39 In these circumstances, it must be assumed that the administrator of a fan page on Facebook, such as the Wirtschaftsakademie, helps to determine for what purpose and with what aids personal data is processed about the users of the fan page, by making settings depending on e.g. . the target group as well as the goals of managing and advertising its activities. For this reason, in this case, the administrator, together with Facebook Ireland, must be classified as a controller within the EU within the meaning of Article 2 (d) of Directive 95/46.

40 The fact that the administrator of a fan page uses the Facebook platform and uses the services associated with it does not relieve the administrator of his obligations with regard to the protection of personal data.

41 It should also be emphasized that the fan pages on Facebook can also be visited by persons who are not Facebook users and who thus do not have a user account on this network. In this case, the administrator of a fan page's responsibility for the processing of these persons 'personal data seems even more important, as the users' mere consultation of the fan page automatically triggers a processing of their personal data.

42 In those circumstances, the recognition that the company operating a social network and the administrator of a fan site on that network share a common responsibility in the processing of the personal data of the users of that fan site helps to ensure a more complete protection of those rights. , which the users of such sites have, in accordance with the requirements of Directive 95/46.

43 However, as the Advocate General observes in points 75 and 76 of his Opinion, it must be made clear that the existence of joint responsibility does not necessarily mean that the various operators involved in the processing of personal data have the same responsibility. On the contrary, the various operators may be responsible for the processing of personal data at different levels and to different extents, so that the individual level of responsibility must be assessed taking into account all the relevant

circumstances of the case.

44 In the light of the foregoing considerations, the answer to the first and second questions must be that Article 2 (d) of Directive 95/46 must be interpreted as meaning that the term 'controller' within the meaning of that provision includes the administrator of a fan page on a social network. network."

In Case C-40/17 Fashion ID, the European Court of Justice has elaborated on its interpretation of joint data liability as set out in the Data Protection Regulation:

67 Since, moreover, Article 2 (d) of Directive 95/46 expressly provides that the term 'controller' includes the body which 'alone or together with others' decides for what purpose and by what means: must be processed personal data, this concept does not necessarily refer to a single body and may relate to several actors participating in this processing, and therefore they are all subject to the applicable provisions on data protection (cf. in this direction judgment of 5.6.2018, Wirtschaftsakademie Schleswig-Holstein, C-210/16, EU: C: 2018: 388, paragraph 29, and of 10.7.2018, Jehovah todistajat, C-25/17, EU: C: 2018: 551, paragraph 65).

68 The Court has also held that a natural or legal person who, for his own purpose, has an influence on the processing of personal data and therefore participates in the determination of the purposes and means of such processing may in turn be regarded as the controller within the meaning of Article 2 (d) of Directive 95/46 (Judgment of 10.7.2018, Jehovah todistajat, C-25/17, EU: C: 2018: 551, paragraph 68).

69 In addition, a joint responsibility of several actors for the same processing as referred to in this provision does not presuppose that each of them has access to the personal data in question (see in this direction judgment of 5.6.2018, Wirtschaftsakademie Schleswig-Holstein, C-210 / 16, EU: C: 2018: 388, paragraph 38, and of 10.7.2018, Jehovah todistajat, C-25/17, EU: C: 2018: 551, paragraph 69).

70 Since the purpose of Article 2 (d) of Directive 95/46 is, by a broad definition of the term 'controller', to ensure the effective and complete protection of the persons concerned, the existence of joint liability does not necessarily imply: that different actors have the same responsibility for the same processing of personal data. On the contrary, the various actors may be responsible for the processing of personal data at different levels and to varying degrees, so that the individual level of responsibility must be assessed taking into account all relevant circumstances in the case (cf. in this direction judgment of 10.7.2018, Jehovah todistajat, C -25/17, EU: C: 2018: 551, paragraph 66).

[…]

74 It follows that, as the Advocate General essentially states in point 101 of his Opinion, a natural or legal person may be the sole controller within the meaning of Article 2 (d) of Directive 95/46 together with others. for processing operations relating to personal data, if that person has a say in the purpose and means of such operations. On the other hand, and without prejudice to any liability under national law in this respect, that natural or legal person may not be deemed to be the controller within the meaning of that provision, for operations which occur before or after the series of proceedings and in respect of which: the person in question neither defines purpose nor aids.

75 Subject to the review by the national court, it is apparent in the present case from the file available to the Court that, by integrating the 'likes' button from Facebook on its website, the Fashion ID having given Facebook Ireland the opportunity to collect personal information about the site's visitors, which arises from the time the person consults the site, and this takes place regardless of whether these visitors are members of the social network Facebook, whether they have clicked on » like the «button from Facebook, or if they are aware that such an operation is taking place.

76 In the light of that information, it must be stated that the processing operations relating to personal data for which Fashion ID, together with Facebook Ireland, can determine the purposes and aids, as defined by the term 'processing of personal data' in Article 2 (b) of Directive 95 / 46 is the collection and disclosure by transmission of personal information relating to visitors to the Fashion ID website. With regard to the said information, on the other hand, it seems immediately impossible for Fashion ID to determine for what purposes and with what aids processing operations concerning personal data are subsequently carried out by Facebook Ireland after their transmission to this company, so Fashion ID can not be considered the data controller for these operations within the meaning of Article 2 (d) of that Directive.

77 As regards the aids used for the collection and transmission of certain personal data concerning the visitors to the Fashion ID website, it is clear from paragraph 75 of this judgment that Fashion ID appears to have integrated the 'like' button from Facebook, as Facebook Ireland makes available to operators of websites, on its website, as Fashion ID was aware that this button is a means of collecting and transmitting the personal information of this website's visitors, regardless of whether they are members of the social network Facebook.

78 In addition, by integrating such a social module on its website, Fashion ID has a decisive influence on the collection and transmission of the website visitors' personal data to the provider of said module, in the present case Facebook Ireland, which

would not have taken place if said module had not been integrated into the site.

79 Against this background, and subject to the verification required by the national court in that regard, it must be assumed that Facebook Ireland and Fashion ID jointly determine the means used for the collection and transmission of Fashion ID's websites. visitors' personal information.

80 As regards the purpose of the said personal data processing operations, it appears that Fashion ID's integration of the 'like' button from Facebook on its website enables the company to optimize the marketing of its products by making them more visible on it. social networking Facebook when a visitor to the site clicks on said button. It is in order to be able to take advantage of this commercial advantage, which consists in increased publicity of its products, that Fashion ID, by integrating such a button on its website, seems to have given consent, at least implicitly, to the collection and disclosure by transmission. of the personal data of its website visitors, as these operations involving the processing of personal data take place in the financial interest of both Fashion ID and Facebook Ireland, the latter having access to this information for the purpose of self-marketing is the consideration for the benefit provided by Fashion ID.

81 Subject to the verification which the national court is required to carry out, it may in that context be assumed that Fashion ID and Facebook jointly determine the purposes for which operations may be carried out for the collection and transmission of the cases in the main proceedings. personal data referred to.

82 As is clear from the case-law cited in paragraph 69 of this judgment, the fact that the operator of a website, such as Fashion ID, does not itself have access to the personal data collected and transmitted to the social module provider with whom the operator jointly determines the purposes and means by which personal data may be processed does not preclude that operator from being 'the controller' within the meaning of Article 2 (d) of Directive 95/46.

[…]

84 Consequently, it appears that Fashion ID may be regarded as the controller within the meaning of Article 2 (d) of Directive 95/46 in conjunction with Facebook Ireland for the collection and transmission of the personal data transmitted to the site's visitors.

85 In view of all the above considerations, the answer to the second question is that the operator of a website, such as Fashion ID, which integrates on this website a social module that enables the website visitors' browser to request content from the provider of this module and in In this connection, the transfer of the visitor's personal data to the said provider may be

considered to be the controller within the meaning of Article 2 (d) of Directive 95/46. However, this responsibility is limited to the operation or series of operations involving the processing of personal data, for which or which this operator actually determines for what purpose and in what way this may take place, ie. the collection and transfer of personal data in the main proceedings. "

4.3. Basis for treatment

The conditions for the lawful processing of personal data are set out in Article 6 of the Data Protection Regulation, which reads as follows:

"Treatment is only lawful if and to the extent that at least one of the following conditions applies:

a) The data subject has given consent to the processing of his personal data for one or more specific purposes.

(b) Processing is necessary for the performance of a contract to which the data subject is a party or for the implementation of measures taken at the request of the data subject prior to the conclusion of a contract.

c) Processing is necessary to comply with a legal obligation incumbent on the data controller.

d) Processing is necessary to protect the vital interests of the data subject or another natural person.

e) Processing is necessary for the purpose of performing a task in the interest of society or which falls within the exercise of public authority, which has been assigned to the data controller.

(f) Processing is necessary for the data controller or a third party to pursue a legitimate interest, unless the data subject's interests or fundamental rights and freedoms requiring the protection of personal data take precedence, in particular if the data subject is a child.

The first subparagraph, point (f), shall not apply to processing carried out by public authorities in the performance of their tasks. "

Consent of the data subject is defined in Article 4 (11) of the Data Protection Regulation as any voluntary, specific, informed and unambiguous expression of the data subject's consent, whereby the data subject agrees by declaration or clear confirmation that personal data relating to the data subject shall be made for treatment.

Recital 32 in the preamble to the Data Protection Regulation states the following:

"Consent should be given in the form of a clear confirmation, which involves a voluntary, specific, informed and unambiguous expression of will from the data subject, whereby the person in question accepts that personal data about the person in

question is processed, e.g. by a written statement, including electronic, or an oral statement. This can e.g. take place by ticking a box when visiting a website, by choosing technical options for information society services or another statement or action that clearly indicates in this connection the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-checked fields or inactivity should therefore not constitute consent. Consent should cover all treatment activities performed for the same purpose or purposes. When treatment serves several purposes, consent should be given to all of them. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily interfere with the use of the service to which consent is given. "

Furthermore, recital 42 in the preamble to the Data Protection Regulation states:

“If processing is based on the data subject's consent, the data controller should be able to demonstrate that the data subject has given consent to the processing. In particular in connection with written declarations of other matters, guarantees should ensure that the data subject is aware of that and to what extent consent has been given. In accordance with Council Directive 93/13 / EEC […], a statement of consent drawn up by the controller should be made available in an easy-to-understand and accessible form and in clear and simple language and should not contain unreasonable conditions. In order to ensure that the consent is informed, the data subject should at least be aware of the data controller's identity and the purposes of the processing for which the personal data are to be used. Consent should not be considered as given voluntarily if the data subject does not have a real or free choice or can not refuse or withdraw his consent without it being to the detriment of the person concerned. "

Finally, page 19 of the Article 29 Working Party's Guidelines on Consent pursuant to Regulation 2016/679, WP 259 rev.01, as adopted by the European Data Protection Board, states:

In any case, consent must always be obtained before the data controller initiates the processing of personal data for which the consent is to be used. The group has consistently stated in its previous statements that consent must be given prior to the treatment activity. Although the Data Protection Regulation does not explicitly provide in Article 4 (1) 11, that consent must be given prior to the treatment activity, this is clearly implied. The title of Article 6 (1) And the wording "has given" in Article 6 (1). 1 (a) supports this interpretation. It follows logically from Article 6 and recital 40 that a valid legal basis must be in place before data processing can begin. Therefore, consent must be given prior to the treatment activity. In principle, it may be sufficient to request the data subject's consent once. However, the data controller must obtain a new and specific consent if the purposes

of the data processing change after obtaining the consent, or if it is intended to use the data for other purposes. "

The processing of personal data must also always be carried out in accordance with the basic principles of Article 5 of the Data Protection Regulation, of which, inter alia: the following appears:

"Personal information must:

(a) treated lawfully, fairly and in a transparent manner in relation to the data subject ('legality, fairness and transparency');

(b) collected for express and legitimate purposes and must not be further processed in a manner incompatible with those purposes; further processing for archival purposes in the public interest, for scientific or historical research purposes or for statistical purposes in accordance with Article 89 (2); Shall not be deemed to be incompatible with the original purpose ('purpose limitation')

(c) be adequate, relevant and limited to what is necessary for the purposes for which they are being processed ('data minimization');

(d) be accurate and, where necessary, updated; every reasonable step must be taken to ensure that personal data which are inaccurate in relation to the purposes for which they are processed are immediately deleted or rectified ('accuracy');

(e) stored in such a way that it is not possible to identify the data subjects for a longer period than is necessary for the purposes for which the personal data in question are processed; personal data may be stored for a longer period if the personal data are processed solely for archival purposes in the public interest, for scientific or historical research purposes or for statistical purposes in accordance with Article 89 (1). Provided that the appropriate technical and organizational measures required by this Regulation are implemented in order to safeguard the data subject's rights and freedoms ('storage restriction');

(f) processed in a manner that ensures adequate security of the personal data concerned, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ("integrity and confidentiality"). "

5. Justification for the Danish Data Protection Agency's decision

5.1. Is this a processing of personal data that the Danish Data Protection Agency has competence to assess?

The Danish Data Protection Agency on the basis of Google's documentation, which is described in more detail in section 2.3, on the basis that the information that is transferred to Google, i.a. includes information about the visitors 'IP address, the website where the Google ad is embedded, the visitors request access to, the date of the request, and information about

online identifiers contained in cookies that Google has stored in the visitors' browser.

The opinion of the Article 29 Working Party on the concept of personal data states that an "element of purpose" may be responsible for the existence of information "about" a particular person. There is an "element of purpose" when the information is used or can be expected to be used for the purpose of assessing a person, treating the person in a certain way or influencing the person's status or behavior.

Furthermore, the opinion of the Article 29 Working Party on Behavioral Marketing states that the information collected for the purpose of behavioral marketing makes it possible to "identify" data subjects, even if their real names are not known. The information collected relates to the data subject's characteristics or behavior, and the information is used to influence the person in question.

In this connection, it appears from Google's documentation that the information i.a. is used for "[personalizing content and ads that you see on Google and on our partners' websites and applications]".

Overall, the Data Inspectorate's assessment is that the information in question about the visitors to dmi.dk, which is collected and transmitted to Google, constitutes personal information about these, as the information relates to the data subject's characteristics and behavior and is used to process the person in question on a specific way in relation to which ads are displayed for that person.

As described above in section 3, the supervision of rules on the processing of personal data, which has not been replaced by special rules implementing the e-Data Protection Directive, lies with the Danish Data Protection Agency.

It is the Data Inspectorate's opinion that in this case only information about cookie identifiers [7] is stored in the end user's terminal equipment and to which Google (via dmi.dk) obtains access.

It is thus the Data Inspectorate's assessment that only a subset of the information that is collected and transmitted to Google is within the scope of application of section 3 (1) of the Executive Order on Cookies. 1, and which thus falls under the Danish Business Authority's supervisory competence. It is in particular the information contained in cookies that Google has stored in the complainant's browser, including in particular the information on cookie identifier (s).

However, the information transmitted to Google is not limited to the information stored in the terminal equipment (cookie identifiers). Information is also collected and transmitted on e.g. the visitors' IP address and other information as described above.

As this additional information constitutes personal data about the visitors, the Danish Data Protection Agency assesses that the Authority has the competence to assess whether the processing of this other personal data about the visitors collected and transmitted to Google takes place in accordance with the Data Protection Regulation and the Data Protection Act.

5.2. Data responsibility

The question then is whether DMI can be considered to be the data controller - possibly jointly with Google - for the processing of the personal data in question.

By integrating content from Google into its website, DMI has provided Google with the ability to collect personal information about the website's visitors, which arises from the time they visit the website.

In view of this, the Danish Data Protection Agency finds that it can be established that the processing operations for which DMI, together with Google, can determine the purposes and aids, are the collection and disclosure of personal information concerning the visitors to dmi.dk.

With regard to the information in question, on the other hand, it seems out of the question for DMI to determine for what purposes and by what means processing operations concerning personal data are subsequently carried out by Google after their transmission thereto, so DMI can not be considered the data controller for these operations. .

With regard to the aids used for the collection and transmission of certain personal information concerning the visitors to dmi.dk, it appears from section 2.2. That DMI has integrated banner ads from Google, which Google makes available to operators of websites, on its website and that DMI is aware that these banner ads, in addition to displaying ads, also collect and transmit personal information about the website's visitors.

By integrating these banner ads on its website, DMI has a decisive influence on the collection and transmission of personal data about the website visitors to Google, as these processing operations would not have taken place if the banner ads had not been integrated on the website. [8]

Against this background, in the Data Inspectorate's view, it must be possible for DMI and Google to jointly determine which aids are used for the collection and transfer of personal information about the visitors to dmi.dk.

As regards the purpose of processing the personal data in question, it can be assumed that DMI's integration of the banner ads from Google on its website is for the purpose of advertising revenue.

By integrating these advertisements on its website, DMI has consented, at least implicitly, to the collection and disclosure of

personal information about the website visitors, as these operations take place in the financial interest of both DMI and Google, the latter having access to this information with for the purpose of evaluating and determining the interests, personal preferences and behavior of the data subjects contribute to the streamlining of the Google advertising network, which also benefits DMI in the form of increased advertising revenue. [9]

On that basis, in the opinion of the Danish Data Protection Agency, it can be assumed that DMI and Google together determine for what purposes the personal data in question has been collected and passed on.

As is clear from Case C-210/16 Wirtschaftsakademie and C-40/17 Fashion ID, paragraphs 69 and 82 respectively, the fact that DMI does not itself have access to the personal data collected and transferred to Google , with whom DMI jointly determines for what purposes and with what aids personal data may be processed, does not prevent DMI from being the data controller.

5.3. Basis for treatment

5.3.1. Who should provide a treatment basis?

First, it must be clarified which of the joint data controllers is to provide a valid processing basis for the initial processing operations in the form of collection and transmission by transmission.

While DMI and Google are jointly responsible for the initial processing operations in the form of collection and transmission by transmission, DMI is only obliged to ensure a valid processing basis for the processing operations for which DMI is co-responsible, ie collection and transmission by transmission. DMI is thus not responsible for processing carried out by Google, including any profiling, etc., which takes place after the collection and transfer in question.

When the processing of personal data about the visitors is triggered by a visit to dmi.dk, it must consequently be the responsibility of DMI and not Google to ensure a valid processing basis.

In cases where the relevant basis for processing is the data subject's consent, this consent must be given before the processing of personal data takes place.

It is noted in this connection that the European Court of Justice in its judgment of 29 July 2019 in case C-40/17 Fashion ID i.a. has also stated that it would not be in accordance with effective and timely protection of the data subject's rights if the consent was given only to the joint controller, who is only later involved, ie. Google.

5.3.2. What is the relevant basis for treatment?

As stated above, the processing of personal data is only lawful if one of the conditions of Article 6 of the Data Protection

Regulation applies, and it is therefore relevant to identify which processing basis (s) are relevant in the present case.

In the light of the facts of the case, in particular Article 6 (1) of the Regulation 1, letters a, e and f, to be relevant to consider as a possible basis for treatment.

To letter f)

DMI is part of the Ministry of Climate, Energy and Supply and thus part of the public administration.

Public authorities may not process personal data as part of the performance of their tasks under Article 6 (1) (f) of the Regulation. As stated above, Article 6 (1) of the Regulation provides: 1, 2nd paragraph.

To letter e)

It is the Data Inspectorate's assessment that the processing of personal data in question, which consists of the collection and transfer of personal data to Google, is not necessary for the performance of a task in the public interest or which falls within DMI's exercise of authority, and the processing can therefore not take place in pursuant to Article 6 (1) of the Regulation 1, letter e.

The Danish Data Protection Agency has hereby placed decisive emphasis on the fact that it is possible for DMI to discontinue the embedded advertisements, so that no personal data about the visitors on dmi.dk is processed, after which the visitors will continue to see banner advertisements, which, however, will not be personalized on the basis of their personal data.

To letter a)

It is against this background that the Danish Data Protection Agency's assessment is that the relevant processing basis for the processing of personal data in question is Article 6 (1) of the Regulation. 1, letter a, on the data subject's consent.

5.3.3. Is a valid consent obtained?

In its assessment of whether a valid consent is obtained, the Danish Data Protection Agency assumes that DMI obtains consent for the processing of personal data at the same time and through the same implemented consent solution as the one concerning consent for placement and reading of cookies on visitors' equipment.

Ad voluntarily

The purpose of the condition of voluntariness is to create transparency for the data subject and give the data subject a choice and control over his personal data. A consent is therefore not considered to have been given voluntarily if the data subject is unable to make a real and free choice.

A service may include multiple processing operations for more than one purpose. An important element in the assessment of whether a consent is voluntary is therefore also the principle of "granularity". The principle implies that in the case of treatments that serve several purposes, separate consent must be obtained for each individual purpose. In the context of data protection law, the division (granulation) of purpose is thus essential to ensure the data subject's control over his information and transparency in relation to which processing operations take place.

DMI's statement of 12 February 2019 shows a screenshot of the implemented consent solution, where at the first interaction there are two options; "OK" and "Show details". The solution also states that:

”DMI and third parties use cookies to make dmi.dk more usable, give you a better experience and for targeted marketing. By clicking OK here you give your consent to this. You can always withdraw your consent. Read more in our privacy policy. ”

It is the Data Inspectorate's assessment that the sub-operations to which a visitor by choosing “OK” gives consent constitute several different treatment purposes. In the opinion of the Danish Data Protection Agency, personal data is thus processed for various purposes, including:

collection of personal information with a view to generating statistics on how visitors use dmi.dk,

behavioral marketing, where the collection of personal information takes place in order to follow the visitors across websites with a view to personalizing ads to the individual visitor through profiling.

It is thus the Data Inspectorate's assessment that the collection of personal data for various purposes on the basis of a single consent does not give visitors a sufficient free choice in relation to being able to identify and select or deselect which purposes the visitor actually wishes to give his consent to. .

The Danish Data Protection Agency has noted that it is possible to select or deselect the collection of personal data for various purposes by selecting "Show details", but that this option is located "one-click-away", and it is thus not possible with it initial interaction with the consent solution.

Ad informed

In order to ensure that the consent is informed, the data subject should at least be aware of the data controller's identity and the purposes of the processing for which the personal data are to be used.

The information to be provided to the data subject must be provided in a simple, easy-to-understand and easily accessible form, and the information must be provided to the data subject before consent is given.

The implemented consent solution on dmi.dk shows which cookies are used on the website, and these are divided into different categories. It also appears from the category "Marketing" that i.a. cookies from the provider DoubleClick are used, and that the purpose of this is “online marketing by collecting information about the users and their activity on the website. The information is used to target advertising to the user across different channels and devices. ”

It is the Data Inspectorate's assessment that the consent that DMI obtains through the implemented solution is not sufficiently informed.

In particular, the Danish Data Protection Agency has emphasized that there is insufficiently clear information about the (joint) data controllers, including Google, in collaboration with whom personal data is collected and to which personal data is passed, and that it is not sufficiently clear to the data subject which personal data collected and transmitted to these (joint) data controllers, including Google.

In this connection, the Danish Data Protection Agency is of the opinion that - with regard to consent to the processing of personal data - it is necessary that a consent solution or declaration in an easily understandable and easily accessible form and in a clear and simple language states which data controllers, for example, personal information is passed on to. It should be noted below that it is the identity of the data controller organization that must appear, and not the data controller's websites, nicknames or product names that the data controller uses, as it is not easy to understand and easily accessible to the data subject.

Ad the structure of the consent solution

Of the basic principle of Article 5 (1) of the Regulation 1, letter a, on legality, reasonableness and transparency, follows in the Data Inspectorate's view that it should be as easy to refrain from giving consent to the processing of personal data as it is to give it.

It is the Data Inspectorate's assessment that the current structure of DMI's consent solution, where the visitor at the first visit is presented with two choices in relation to the processing of personal data; "OK" and "Show details" do not meet this transparency requirement.

The Danish Data Protection Agency has hereby emphasized that it is not possible for a visitor to the website to refuse the processing of personal data during the initial visit to dmi.dk. This requires the visitor to select "Show Details" and then select "Update Consent". In the opinion of the Danish Data Protection Agency, such an "one-click-away" approach is not transparent,

as it requires an extra step for the data subject to refuse to give consent to the processing of personal data, and it is not clear to the data subject that it is possible to omit to give consent to the processing of personal data by selecting "Show details", just as the wording "Update consent" may give rise to confusion.

Similarly, in the Data Inspectorate's view, it is not in accordance with the principle of transparency that the possibility of refraining from giving consent to the processing of personal data in DMI's solution does not have the same message effect - that is, it is not as clear - as the possibility of to give consent, whereby the data subject is indirectly pushed in the direction of giving consent to the processing of personal data.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC (General data protection regulation).

[2] https://policies.google.com/technologies/partner-sites?hl=en-GB

[3] https://policies.google.com/technologies/ads?hl=en-GB

[4] https://policies.google.com/privacy/key-terms?hl=en-GB#toc-terms-server-logs

[5] Article 29 Working Party Opinion No 4/2007 on the concept of personal data, p. 10f.

[6] Article 29 Working Party Opinion No 2/2010 on Behavioral Advertising on the Internet, p. 9f.

[7] In Google's own example mentioned in section 2.3. above, the cookie identifier is "740674ce2123e969"

[8] Judgment of the European Court of Justice of 29 July 2019 in Case C-40/17 Fashion ID, paragraph 78.

[9] Judgment of the European Court of Justice of 29 July 2019 in Case C-40/17 Fashion ID, paragraph 80.