The Danish Data Protection Authority criticizes the automatic filling in of information when purchasing on a website

Date: 13-12-2021

Decision

Private companies

Criticism

Injunction

Complaint

Unintentional disclosure

Treatment safety

Basis of treatment

The Danish Data Protection Authority has made a decision in a case concerning Rito ApS' processing of personal data in connection with the automatic filling in of personal data about customers when purchasing on the company's website.

Journal number: 2020-31-3611

Summary

Rito Aps uses a function on the website www.rito.dk where, by entering an already known e-mail address, a number of fields are automatically filled in with personal data, including name, address and telephone number, which have previously been used in connection with e- the email address. The use of automatic filling does not require that you have logged in beforehand or otherwise identified yourself.

By entering e-mail addresses of previous customers, other unauthorized users could thus potentially access information about them.

After the case had been submitted to the Data Council, the Danish Data Protection Authority stated that Rito ApS, by using a functionality whereby information about previous customers could potentially be accessed by other unauthorized users, did not meet the requirements for an appropriate level of security in Article 32 of the Data Protection Regulation.

The supervisory authority laid, among other things, emphasis on the fact that any passing on of personal data about former customers to other users of the website was not originally intended - i.e. that it was not the purpose of the solution that users should have access to information about other customers.

The Norwegian Data Protection Authority also found that Rito ApS's new solution, where customers had to accept that the company saved the information for later automatic address filling, still did not meet the requirements for an appropriate level of security, since, in the opinion of the Danish Data Protection Authority, you cannot waive the necessary security by to give consent.

Against this background, the Danish Data Protection Authority found grounds to express criticism that Rito ApS's processing of personal data had not taken place in accordance with the rules in the data protection regulation.

The Danish Data Protection Authority also ordered Rito ApS to stop using automatic filling in of personal data about customers when purchasing on the company's website - regardless of whether some form of acceptance had been obtained from the customers or not.

Autofill can be done within the rules

In continuation of the case, the Danish Data Protection Authority found reason to consider whether – within the framework of Article 32 of the Data Protection Regulation – it is possible for companies to use a solution that automatically fills in information about users on a website.

In this connection, it is the Danish Data Protection Authority's immediate assessment that solutions with auto-filling of information, where the data subject has previously verified himself sufficiently in another way, for example via a unique log-in on the website, will meet the security requirements in Article 32 of the Data Protection Regulation .

1. Decision

After a review of the case, the Danish Data Protection Authority finds - after the case has been submitted to the Data Council - that there is a basis for expressing criticism that Rito ApS' processing of personal data has not taken place in accordance with the rules in the data protection regulation[1] article 32.

2. Injunction

The Danish Data Protection Authority also orders Rito ApS to cease using the auto-fill functionality described by Rito ApS, which applies regardless of whether a form of acceptance has been obtained from the customers or not.

The order is announced in accordance with the data protection regulation, article 58, subsection 2, letter d.

The deadline for compliance with the order is 3 weeks from today's date.

The Danish Data Protection Authority must request, no later than the same date, to receive confirmation that the order has

been complied with.

The Norwegian Data Protection Authority draws attention to the fact that according to the Data Protection Act section 41, subsection 2, no. 5, it is a criminal offense to fail to comply with an order issued by the Danish Data Protection Authority in accordance with Article 58, subsection of the Data Protection Regulation. 2, letter d.

Below follows a closer review of the case and a rationale for the Data Protection Authority's decision.

3. Case presentation

It appears from the case that Rito ApS on the website, www.rito.dk, uses a functionality where when entering an e-mail address already known to the solution, a number of fields are automatically filled in with information about name, address and telephone number, that has previously been used in connection with the e-mail address in question. The use of automatic filling does not require that you have logged in beforehand or otherwise identified yourself.

It also appears from the case that, during the processing of the present case, Rito ApS has added an option for new customers to opt in and out of the functionality. Thus, the functionality with automatic filling is de-selected by clicking on a – previously ticked – check box with the accompanying text:

"I agree to use automatic address completion on my future orders.

In this way, my personal information is retrieved via the e-mail address I entered on my last order. The information collected is the following: full name, address and telephone number. Please note that if others know your e-mail address, they will also have access to the above information via this function. You can always withdraw your consent again."

3.1. Complainant's comments

The complainant has generally referred to the fact that the site www.rito.dk automatically fills in information about name, address and telephone number when you enter an e-mail address already known to the website solution in connection with trading on the site. In this connection, the complainant has stated that it is thus possible to extract information about the name, address and telephone number of any customer simply by entering the relevant e-mail address.

3.2. Rito ApS' comments

Rito ApS has generally stated that the procedure in question, whereby any information about name, address and telephone number is found automatically, follows a completely common industry standard, which is used by many web shops throughout Denmark, the Nordics and the rest of Europe. The information is collected on the basis of previously completed transactions on

the website.

Rito ApS has also stated that you must have knowledge of a person's e-mail address in order to access other information linked to the e-mail address in question, and that only ten postings can be made from the same IP address within 24 hours . In addition, Rito ApS has stated that the company's system monitors irregular behaviour, which is then blocked.

Rito ApS has stated that the solution has been risk assessed, although not in writing, and that the company considers it highly unlikely that the information could come to the knowledge of unauthorized persons in connection with the solution, as Rito ApS only processes general personal data, which according to Rito ApS can most often be retrieved on other pages if you know a person's e-mail address.

Furthermore, Rito ApS has stated that, based on the present request, the company has reconsidered the automated solution and decided to let it run in its current form, albeit with the change that the individual customer must accept that the company saves the information for later automatic address filling .

4. Reason for the Data Protection Authority's decision

4.1. The Danish Data Protection Authority assumes that the processing of personal data about names, addresses and telephone numbers, which takes place via the mentioned automatic filling, is carried out with a view to providing an easier and faster purchase process for the individual customers of Rito ApS.

Furthermore, the Danish Data Protection Authority assumes that any passing on of personal data about former customers to other users of the website is not intended as a starting point - i.e. that it is not the purpose of the solution that users should have access to information about other customers. In this connection, the supervisory authority has noted that Rito ApS has, according to the information, implemented certain measures with a view to preventing abuse of access to auto-completed information, including a restriction to make a maximum of ten postings from the same IP address within 24 hours and monitoring of irregular behavior.

Article 32, subsection of the Data Protection Regulation. 1, states that the data controller, taking into account the current technical level, the implementation costs and the nature, scope, context and purpose of the processing in question as well as the risks of varying probability and seriousness to the rights and freedoms of natural persons, implements appropriate technical and organizational measures in order to ensure a level of security appropriate to these risks. It also follows from Article 32, subsection 1, letter b, that the data controller, depending on what is relevant, i.a. must ensure continued

confidentiality of processing systems and services.

Furthermore, it follows from the data protection regulation article 32, subsection 2, that the data controller, when assessing which level of security is appropriate, must take into account the risks posed by processing, e.g. unauthorized disclosure of personal data.

The Danish Data Protection Authority is of the opinion that it follows from the requirement for adequate security, cf. Article 32, that a company when using an automatic filling functionality has a duty to ensure the confidentiality of customer information – i.e. ensure that information about customers does not come to the knowledge of unauthorized parties. This applies regardless of whether the personal data belongs to the special categories or not.

In extension of this, the Danish Data Protection Authority finds that Rito ApS, by using the functionality in question, whereby information about previous customers can potentially be accessed by other unauthorized parties, has not met the requirements for an appropriate level of security in Article 32 of the Data Protection Regulation.

In this connection, the Data Protection Authority must note that by entering an e-mail address at www.rito.dk, depending on the circumstances, it will be possible to access information about persons with name and address protection, just as it will be possible to provide information that can potentially be used for targeted phishing. Unauthorized access to more data means, among other things, that the probability of successful phishing increases, e.g. by using name, address and information that the customer has shopped via the website.

4.2. The Danish Data Protection Authority has noted that Rito ApS, based on the Danish Data Protection Authority's inquiry in the case, has reconsidered the solution and decided to let it run in its current form, however with the change that the individual customer must accept that the company saves the information for later automatic address filling.

On the basis of the information provided, however, the Danish Data Protection Authority is of the opinion that the relevant information to the customers and their possible acceptance does not increase the security of the processing of the data subjects' information. In the opinion of the supervisory authority, a data subject cannot waive that processing takes place with the necessary security and therefore not by consent allow a level of security that does not meet the requirements of Article 32 of the data protection regulation. meets the requirements for an appropriate level of security in Article 32 of the Data Protection Regulation.

On the contrary, the Danish Data Protection Authority is of the opinion that Rito ApS's new solution for obtaining consent can

contribute to increasing attention to the lack of security, which in itself can lead to an increased risk of abuse.

The Danish Data Protection Authority is therefore of the opinion that Rito ApS's current solution is also in breach of Article 32 of the Data Protection Regulation.

After a review of the case, the Danish Data Protection Authority finds that there are grounds for expressing criticism that Rito ApS's processing of personal data has not taken place in accordance with the rules in Article 32 of the Data Protection Regulation.

The Danish Data Protection Authority also orders Rito ApS to cease using the auto-fill functionality described by Rito ApS, which applies regardless of whether a form of acceptance has been obtained from the customers or not.

4.3. In continuation of the above, the Danish Data Protection Authority has found reason to consider whether – within the framework of Article 32 of the Data Protection Regulation – it is possible for companies to use a solution that automatically fills in information about users on the data controller's website.

The Danish Data Protection Authority is aware that auto-filling of information on a website can be a user-friendly and business-efficient way of handling e.g. form filling on.

In this connection, it is the Danish Data Protection Authority's immediate assessment that solutions with auto-filling of information, where the information is only entered after the registered person has verified himself sufficiently in another way, for example via a unique log-in on the website, use of a certificate, or other form of unambiguous identification, will be able to meet the security requirements in Article 32 of the Data Protection Regulation.

The Danish Data Protection Authority cannot rule out that it will be possible to establish other types of solutions where auto-filling is used without prior log-in or other form of verification of the data subject. However, the supervisor must note that the data controller is responsible for and must be able to demonstrate and document that personal data is processed in a way that ensures sufficient security for the personal data in question. It is thus the data controller's responsibility to meet the requirements for adequate security according to Article 32, and it is, as mentioned, the Danish Data Protection Authority's opinion that the requirements for adequate security cannot be waived with the data subject's consent.

When assessing what is appropriate security, the data controller must be particularly aware of risks for the data subject, especially if the access to autofill additional information is generally known or easily accessible information, e.g. an email address or phone number. Such generally known or easily accessible information will, firstly, make it easier for unauthorized

persons to access the auto-completed information, just as - depending on the circumstances via simple searches on the internet - a basis can be created for the auto-completed information to be collated with other publicly available information about the data subject, which could increase the risk for the data subject.

The data controller must also consider whether the information that is accessed via auto-filling is information that must be described as particularly worthy of protection, e.g. information about name and address protection, or purchases that in themselves could reveal information of a confidential nature about the customer.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons in connection with the processing of personal data and on the free exchange of such data and on the repeal of Directive 95/46/EC (general regulation on data protection).