Statement

Statement: Encrypting the transmission of same-sex marriage information

Date: 30-09-2021

Decision

Public authorities

Processed by the Data Council

Treatment safety

Sensitive information

Unsafe transmission

After submitting a question from the Family Court to the Data Council, the Data Protection Authority has stated that information that two people of the same sex have applied to enter into marriage in Denmark should not, as a general rule, be considered sensitive personal data, but that it must always be a concrete assessment.

Journal number: 2020-212-2099

Summary

In response to a question from the Family Court, the Data Protection Authority - after submission to the Data Council - among other things took position on whether information that two people of the same sex have applied to enter into marriage in Denmark should be considered sensitive personal data covered by Article 9 of the data protection regulation.

The question arose from the Family Court's assessment of whether the self-service solution that the Family Court makes available to applicants was sufficiently secure if information that two people of the same sex have applied to enter into marriage were to be considered sensitive personal data.

The Danish Data Protection Authority found that, as a starting point, such information should be considered non-sensitive personal data that is only covered by Article 6 of the Data Protection Regulation, but that a specific assessment should always be made.

In this connection, the Danish Data Protection Authority could not rule out that in some cases – for example in countries where marriage between persons of the same sex is prohibited by law or socially condemned – it may be associated with a high risk for data subjects if information that the person has applied to enter into marriage with a person of the same sex came to the

knowledge of an unauthorized person.

Against this background, it was the Danish Data Protection Authority's assessment that the Family Court should consider whether a number of additional security measures should be implemented in the self-service solution, including limiting the information in automatic receipt letters from the self-service solution and the option to opt out of receiving a receipt letter.

Statement

1.

In an inquiry of 10 September 2020, the Family Court has requested the Danish Data Protection Authority's position on whether applications for the conclusion of marriage between two persons of the same sex must be considered to constitute processing of information about the sexual orientation of natural persons, Article 9 of the Data Protection Regulation (1), PCS. 1, and whether the associated sending of e-mails with acknowledgment letters must be encrypted, cf. Article 32, paragraph 1.

2.

It appears from the case that the Family Court uses a self-service solution for submitting applications to enter into marriage in Denmark for international couples, and that in connection with the submission of the application, a letter of acknowledgment is automatically sent to the applicants and their possible representatives.

In this connection, the Family Court has stated that in the self-service solution, i.a. information about the applicants' names and addresses is registered, and that there is a field in the solution where the applicants must state their gender. The information on gender is used to verify whether there is agreement between the information in the application and the information in the applicant's passport, where the gender is also stated.

According to the Family Court, the information about the applicants' gender is not used for other purposes, and the self-service solution thus does not differentiate between whether applicants are of the same or different gender. The Family Court has also stated that no information about the applicants' sexual orientation is otherwise recorded.

Furthermore, the Family Court has stated that no checks are carried out to see if the names are correct or spelled correctly, just as there is no integration between the self-service solution and the CPR register due to the fact that the applicants typically do not have a Danish social security number.

With regard to the receipt letter sent to the applicants in connection with the submission of the application, the Family Court has stated that the letter contains information about the Family Court's case number, name and address of the applicants and

information that the receipt relates to an application for examination certificates with a view to entering marriage in Denmark. Information about the applicants' gender does not appear in the acknowledgment letter.

The Family Court has also stated that most applicants do not have a NemID, and that in these cases the receipt is sent unencrypted to the email addresses that the applicants have entered, often in the form of Gmail, Outlook or similar email addresses.

3.

As far as the information that is sent with automatically generated acknowledgment letters is concerned, it is the Family Court's assessment that it is personal data that is only covered by the article of the data protection regulation.

It is also the Family Court's assessment that it will only be possible to derive information about the applicants' sexual orientation if the information in the receipt letter is compared with additional information - for example knowledge of whether the applicants' names in their countries of residence are female or male names. In this connection, the Family Court is of the opinion that the risk of an outside and unauthorized person using illegal means to gain access to the e-mail accounts of the limited target group and using information in the acknowledgment letter in combination with other information to derive information about the applicants' sexual orientation and with illegal intentions makes use of this knowledge, is very low.

The Family Court thus considers that it is unlikely that the sending of acknowledgment letters to the given e-mail addresses entails any particular risk of negative consequences for the rights of the data subjects, including freedoms.

4.

The Danish Data Protection Authority finds – after the case has been submitted to the Data Council – that information that two people of the same sex have submitted an application to enter into marriage in Denmark must, as a starting point, be considered to be information that is only covered by Article 6 of the Data Protection Regulation However, the Danish Data Protection Authority is of the opinion that such information must always be assessed in light of the purpose of the processing of the information in question and the context in which the information is otherwise included

As the case has been disclosed, however, the Data Protection Authority agrees with the Family Court that the relevant processing of information about e.g. gender in the self-service solution cannot be considered to be a processing of information about natural persons' sexual relationships or sexual orientation, cf. the data protection regulation, article 9, subsection 1. The Norwegian Data Protection Authority has, among other things, emphasized that the purpose of the processing of the

information is not to process information about the applicants' sexual relationships, etc., just as the information about gender is only used to verify whether there is agreement between the information in the application and the information in the applicants' passports.

5.

It follows from Article 32 of the Data Protection Regulation that the data controller and the data processor – 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 for the rights and freedoms of natural persons – carry out appropriate technical and organizational measures to ensure a level of security appropriate to these

The Danish Data Protection Authority has previously stated in several contexts that it follows from the requirement for adequate security, cf. Article 32, that it will normally be an appropriate security measure – for both public and private actors – to use encryption when transmitting confidential and sensitive personal data over networks , over which the data controller has no control.

However, this does not preclude that the data controller must always make a concrete assessment of what will be adequate security for the transmission of information over such networks – that is, also in situations where information is transmitted that is not confidential or sensitive nature. This specific assessment implies, among other things, that the data controller must always identify and deal with relevant risks for the rights of the data subjects, and that the data controller must, in extension, implement appropriate security measures to protect these rights.

In this connection, the Danish Data Protection Authority is of the opinion that the transmission of personal data over networks over which the data controller has no control generally entails a relatively high risk of the information becoming known to unauthorized persons.

As far as the transmission of the acknowledgment letters referred to in this case is concerned, the Danish Data Protection Authority must initially note that the Danish Data Protection Authority does not know in which countries the applicants reside, and that the Danish Data Protection Authority therefore cannot make a concrete assessment of the risks for the applicants in question. rights.

However, in a number of countries - both within and outside the EU - it can be associated with significant risks if it comes to unauthorized knowledge that a marriage has been entered into - or an application has been submitted - between two people of

the same sex. The Danish Data Protection Authority hereby, among other things, emphasis on the fact that in some countries marriages between persons of the same sex may be prohibited by law or associated with such social condemnation that it may entail significant risks for the rights of those registered.

The Danish Data Protection Authority cannot therefore rule out that there may be a high risk for those registered if unencrypted receipt letters come to the knowledge of unauthorized parties, whether this happens during transport or when stored on the mail servers. In this connection, the supervisory authority has noted that acknowledgment letters - in addition to the applicants' names - also contain information about the applicants' addresses, which can potentially increase the risk for those registered.

As the Norwegian Data Protection Authority must emphasize that this opinion is not a departure from the starting point, according to which it will normally be an appropriate security measure – for both public and private actors – to use encryption when transmitting confidential and sensitive personal data via the Internet, the Danish Data Protection Authority must invite the Family Court to consider whether for some data subjects there may be such a high risk that unencrypted transmission of information does not reflect an adequate level of security.

If so, it is the Danish Data Protection Authority's assessment that the Family Court should consider which security measures might be appropriate, including e.g. that the information in acknowledgment letters is limited to such an extent that it is not possible to assess the specific nature of the applications (data minimization), that the registered can opt out of the option of being sent an acknowledgment letter and/or that a solution is established where the information remains on the Family Court's server site and can only be downloaded or accessed via a link and an additional authentication factor on an HTTPS connection with a certificate.

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)