The Danish Data Protection Authority expresses serious criticism of 3F Østfyn

Date: 11-05-2022

Decision

Private companies

Serious criticism

Reported breach of personal data security

Treatment safety

Unintentional disclosure

Basic principles

The Danish Data Protection Authority has expressed serious criticism of 3F Østfyn for not having lived up to the principle of correctness and the requirement for adequate security by inadvertently passing on information about a member to the member's former and violent partner.

Journal Number: 2021-441-9224

Summary

The Danish Data Protection Authority has made a decision in a case where 3F Østfyn has reported a breach of personal data security.

The case is about a member of 3F changing his name and address and getting address protection in the CPR register when he moved away from his violent partner.

3F Østfyn updates the members' names and addresses based on address information from the CPR register. In cases where a member chooses address protection in the CPR register, 3F no longer receives information about e.g. the member's address, and the address field is unlocked in 3F's CRM system, so that the member's information can be maintained manually

In this case, the member contacted 3F Østfyn to update his name and address information, but due to human error, only the name was updated. In connection with the publication of the Fagbladet from 3F, the member's name change was listed in the magazine, but sent to the member's original address, where the former cohabitant continued to reside. Thereby, the former cohabitant became aware of the member's new name.

Processing incorrect information and lack of technical and organizational measures

The Danish Data Protection Authority found grounds for issuing serious criticism when the Danish Data Protection Authority concluded that 3F Østfyn's system was generally set up in such a way that - in given usage scenarios - it would process potentially incorrect information, and that 3F Østfyn had not taken every reasonable step to ensure that the information was deleted or corrected. 3F Østfyn therefore processed personal data contrary to the principle of correctness.

The Danish Data Protection Authority further established that 3F Østfyn had not taken appropriate organizational and technical measures to ensure a level of security that suited the specific risk to the rights of the data subjects, particularly as no procedures or system support had been set up to ensure that the information was updated.

The Danish Data Protection Authority laid, among other things, emphasis that the principle of correctness obliges that systems must not be set up in a way that contributes to the creation and processing of incorrect or incomplete data. In addition, it is essential that the data controller identifies the risks that the specific processing poses for the data subjects. It is not sufficient to simply focus on generic risk scenarios and introduce security measures that protect data subjects against these risks.

Possible solutions for technical and organizational measures

In the decision, the Data Protection Authority has listed possible proposals for technical and organizational measures that could be considered relevant in the specific case.

The CRM system could, for example, is set up with an automatic reaction (warning), which makes the employee aware that there is now name/address protection after the address field has been unlocked in the CRM system, and that the specific employee must check whether the information is correct before the information can is used – e.g. to send out material (blocking all automatic processing of the data in which a change has been registered). This technical measure should be supported by special processes and guidelines for the maintenance and administration of the field values when it is a manually maintained field.

1. Decision

After a review of the case, the Danish Data Protection Authority finds that there are grounds for expressing serious criticism that 3F Østfyn's processing of personal data has not taken place in accordance with the rules in the data protection regulation[1] article 32, subsection 1 and Article 5, subsection 1, letter d.

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

2. Case presentation

On 28 May 2021, 3F Østfyn reported a breach of personal data security to the Danish Data Protection Authority.

It appears from the notification that a member of 3F, when moving out of his violent cohabitant, changes his name and address and receives address protection in the CPR register. In connection with the publication of the Fagbladet from 3F, the member's new name is listed in the magazine, but sent to the address where the former cohabitant still resides, with the consequence that the latter will thus become aware of the member's new name.

It appears from the case that 3F registers name and address information in a CRM system. The purpose of the processing of this information is to take care of the membership of 3F, including in the specific case of publishing the Fagbladet, which is sent to members of 3F.

In relation to 3F Østfyn's procedures for updating members' names and addresses in the CRM system, 3F Østfyn informs that members' names and addresses are updated daily on the basis of address information from the CPR register. The updates are made in 3F's CRM system, which functions as a central source system for use by 3F's departments locally. 3F Østfyn further states that if a member chooses to have address protection in the CPR register, 3F will no longer receive name and address information about this member from the CPR register. In cases where 3F no longer receives address information on a member from the CPR register, the address field in 3F's CRM is unlocked so that the member's current CPR address can be maintained and manually updated locally by 3F's departments.

3F Østfyn has stated that when the address field is unlocked for local updating thereof, until an update of the address field is carried out manually and locally, it will be the last known address in the address field, i.e. the address before the address protection came into effect.

3F Østfyn has stated that the member - without using the CPR register - has contacted 3F Østfyn by e-mail and informed them of the person's new name and address. In the event of a human error in connection with the updating of the member's information, only the member's new name is updated, but not the member's new address and thus the member's new name is linked to the previous address where the member had residence. The magazine has thus been sent using a previous address that has not been corrected, despite the member having made an inquiry and drawing attention to the changes in her contact information.

The Danish Data Protection Authority has noted that 3F Østfyn states that an information campaign will be carried out as well as information and educational activities in 3F Østfyn with a view to raising awareness in relation to ensuring that similar

breaches do not happen again. Furthermore, 3F Østfyn states in their statement that an update will be carried out of 3F Østfyn's internal procedures in relation to handling updates of names and addresses as well as their protection.

3. Reason for the Data Protection Authority's decision

Based on the information provided by 3F Østfyn, the Data Protection Authority assumes that the CRM system uses the last known address as the default value when the member opts for address protection in the CPR register. In addition, it is assumed – in accordance with 3F Østfyn's explanation in this regard – that the department by mistake did not correct the address of the member's new residence, but only the name of the member.

By sending the magazine to the original address, with the member's new name, an unauthorized disclosure of personal data to the former cohabitant took place.

On that basis, the supervisory authority finds that there has been a breach of personal data security, cf. Article 4, No. 12 of the Data Protection Regulation.

3.1. Article 5 of the Data Protection Regulation, subsection 1, letter d

It follows from the data protection regulation's article 5, subsection 1, letter d, that personal data must be correct and, if necessary, updated, and that every reasonable step must be taken to ensure that personal data that is incorrect in relation to the purposes for which it is processed is immediately deleted or corrected

It is the Danish Data Protection Authority's opinion that this principle entails an obligation that the technical support of the business processes must not generally be implemented in a way that creates incorrect data. The principle of data protection in the design of solutions, cf. the data protection regulation's article 25, also requires that the system effectively implements the data protection principles.

It is the opinion of the Danish Data Protection Authority that retention of the original address, in situations where the member chooses to have a protected address in the CPR register, should not be without a secure verification of the member's correctness, should appear from the CRM system. A situation like the present one, where the value for the address is retained by default, creates several possible risk scenarios for the rights of data subjects.

A possible solution scenario would be if the field was either left without a value, or the value was blocked for use, e.g. publication of the trade magazine and it required a positive action to activate the address. This should be supported by special processes and guidelines for maintaining the field value, since in this usage scenario it is a manually maintained field.

By not having such procedures and by using the original address as the value as a system standard, and as it is Datailsynet's opinion that this will systematically result in the processing of incorrect information, 3F Østfyn has not complied with Article 5, subsection 1, letter d .

3.2. Article 32 of the Data Protection Regulation

It follows from the data protection regulation article 32, subsection 1, that the data controller must take and implement appropriate technical and organizational measures to ensure a level of security that matches the risks involved in the data controller's processing of personal data, including e.g. to ensure ongoing integrity (e.g. that information is correct and reliable), cf. Article 32, paragraph 1, letter b.

The data controller thus has a duty to identify the risks that the data controller's processing poses to the data subjects and to ensure that appropriate security measures are introduced to protect the data subjects against these risks.

The Danish Data Protection Authority is of the opinion that the requirement, cf. Article 32, of adequate security will normally mean that in systems with a large number of confidential information about a large number of users, higher requirements must be placed on the care of the data controller in ensuring that there is no unauthorized disclosure of personal data, and that you, as the data controller, ensure that information about registered persons does not come to the knowledge of unauthorized persons. Furthermore, the Norwegian Data Protection Authority considers that appropriate control and handling of information about name and address protection should be carried out, and that this places greater demands on employees' care in connection with the transmission of personal data, including ensuring that this is sent to the correct recipient.

Furthermore, the Danish Data Protection Authority is of the opinion that the requirement in Article 32, point 1, letter b, regarding the processing of correct information will normally mean that the data controller must have established procedures to ensure that information is updated where necessary and correctly, when the data controller becomes aware of the inaccuracy of the information. Furthermore, the Danish Data Protection Authority is of the opinion that data controllers have an obligation to instruct relevant employees about these procedures and, to the extent necessary, to check whether the employees update the information correctly

The Danish Data Protection Authority is of the opinion that organizational measures must be secured against the normally occurring error scenarios. In particular, a breach of personal data security must give rise to reflection on the measures that have been implemented.

There may therefore be a need to implement additional measures to compensate for the human errors.

The CRM system could e.g. is set up with an automatic reaction (warning) which makes the employee aware that there is name/address protection after the address field is unlocked in the CRM system and that the specific employee, before taking further action, must carry out a human control of the members' conditions (for example whether there is name and address protection and whether the information provided is correct.

In order to prevent human errors, such a warning should be present in an IT system and not only described in a procedure, especially in a situation like the present one, where the situation arises from a technical integration. It is generally the opinion of the Danish Data Protection Authority that a data controller – in addition to establishing organizational security measures such as guidelines, procedures, awareness etc. – must establish appropriate technical security measures, if this is necessary to achieve an appropriate level of security.

A possible technical and organizational measure could be that the sending of material to the member is automatically stopped after the receipt of address information from the CPR register has ceased, until an employee has the opportunity to verify the correct address with the member, when the address can no longer be updated via CPR.

In addition, 3F Østfyn should make an assessment of whether a specific procedure for handling the situation where members are both given name and address protection as well as a change of name and address gives rise to a change in the risk assessment of the usage scenario, which requires a mitigating measure that must be drawn up and implemented going forward.

By not having overall taken measures that were appropriate to the specific risk of the processing of the member's information, in connection with both address and name change, at the same time as registering a secret address in the CPR register, 3F Østfyn has not complied with the data protection regulation's article 32, subsection 1.

3.3. Measure

After a review of the case, the Danish Data Protection Authority finds that there are grounds for expressing serious criticism that 3F ØStfyn's system support was set up to process potentially incorrect information and did not sufficiently ensure that the processed information was correct, and that 3F Østfyn has not taken appropriate organizational and technical measures to ensure the updating and correctness of the processed information, cf. the data protection regulation, article 5, subsection 1, letter d, and Article 32, subsection 1.

When choosing a response, the Danish Data Protection Authority emphasized that 3F Østfyn's procedures and workflows were not set up to handle situations regarding name and address protection and where members move in connection with address protection. In the specific situation, we are talking about a member who has made a name change, moved to a new address and received name and address protection. Based on what was stated in 3F Østfyn's statement, handling such an update of the members' information is not described in procedures or by a technical set-up of systems capable of giving an employee a warning about this.

The Danish Data Protection Authority emphasized that when the registered person gets address protection in the CPR register, 3F no longer receives information about the address and the address field in 3F Østfyn's CRM system is unlocked with the last known address, until the manual is updated by an employee in the local departments. In this context, the Danish Data Protection Authority considers it contrary to the principles of data protection law that the address before the address protection came into effect without further ado and without control and verification is used as a basis.

In addition, the Danish Data Protection Authority has emphasized that there is no technical or organizational control in the CRM system that stops all sending of letters/magazines/etc. until the address can be verified, as supplement to the described workflow.

The Danish Data Protection Authority has also emphasized that the missing technical and organizational measures deal with situations where information about name and address protection is concerned. In relation to the technical set-up of the CRM system, 3F Østfyn is not considered to have taken into account the risks and consequences that accidental disclosure will and can entail when processing information about persons with name and address protection.

In addition, the Danish Data Protection Authority has emphasized that the consequences for the data subject in the specific case are considered to be serious, as with this breach of personal data security personal data has been passed on to the person who is the reason why the member has had to change his name and address and obtain name and address protection in the CPR register. In the assessment, the Danish Data Protection Authority has thus placed emphasis on the nature of the information and the consequences that loss of confidentiality may have for the data subjects in these situations, given the consideration behind people's name and address being protected.

As an aggravating circumstance, the Data Protection Authority has placed emphasis on the fact that the member has made an extra effort by informing 3F Østfyn and made special and specific attention to address protection and risks for the data subject

associated with loss of confidentiality of personal data. In conclusion, it is emphasized that the missing and insufficient procedure and workflows for updating protected name and address are considered to be the direct cause of the breach.

3.4. Summary

Based on the above, the Danish Data Protection Authority finds that there are grounds for expressing serious criticism that 3F Østfyn's processing of personal data has not taken place in accordance with the rules in the data protection regulation[2] article 32, subsection 1 and Article 5, subsection 1, letter d.

[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).

[2] 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).