Serious criticism of the Family Court

Date: 06-09-2022

Decision

Public authorities

Serious criticism

Injunction

Supervision / self-management case

Reported breach of personal data security

Notification of breach of personal data security

Unintentional disclosure

Treatment safety

Risk assessment and impact analysis

On the basis of a case initiated on its own initiative regarding the Family Court's accidental disclosure of protected name and address information, the Data Protection Authority expresses serious criticism and issues an injunction.

Journal number: 2021-432-0063

Summary

In autumn 2021, the Danish Data Protection Authority started a case of its own initiative regarding the Family Court's accidental disclosure of protected name and address information to unauthorized persons. The case also included the disclosure of other information about a party's place of residence, e.g. the name of the child's institution.

37 breach of unauthorized disclosure

The Family Court has reported 37 breaches of personal data security to the Danish Data Protection Authority in the period from 27 May 2021 to 16 August 2022, which relate to the fact that the Family Court had unjustifiably passed on information about e.g. one party's protected address to the other party in a case with the authority, where one party had a protected address precisely to avoid the other party getting to know the address.

The Danish Data Protection Authority has previously dealt with a case about the Family Court's accidental disclosure of personal data, which the Danish Data Protection Authority decided on 4 March 2021.

The Danish Data Protection Authority can ascertain that, following the Danish Authority's decision of 4 March 2021, the Family Court has implemented significant measures to avoid accidental disclosure of protected name and address information.

Serious criticism for not meeting the requirement of adequate security

However, the Data Protection Authority also found that the Family Court had not met the requirement for adequate security, as the Family Court, despite having detected and reported several uniform breaches of personal data security, had not reconsidered the existing measures with a view to preventing future breaches of the same type .

The supervisory authority therefore expressed serious criticism that the Family Court's processing of personal data had not taken place in accordance with the rules on processing security.

When choosing a response, the Danish Data Protection Authority emphasized in a stricter direction that it may be associated with major consequences for the registered if their protected address or other place of residence, such as e.g. the name of a shelter, is inadvertently passed on to the person they are trying to hide from.

At the same time, the Data Protection Authority found that there was a basis for ordering the Family Court to carry out a renewed risk assessment based on the 37 breaches of personal data security that the case is about. The deadline for compliance with the order is 6 January 2023.

Decision

The Danish Data Protection Authority hereby returns to the case where, on the basis of a number of reported breaches of personal data security, on 13 October 2021, the Danish Data Protection Authority started a case of its own accord regarding the Family Court's accidental disclosure of protected name and address information.

The Danish Data Protection Authority has subsequently received further reports from the Family Court about similar incidents. The reviews covered by this decision have been received from 27 May 2021 to 16 August 2022 and have the following reference numbers:

cc4946f11f4a6fe895ffff75c6f86013413cfe61

add576ddae85727c50a947fbdca51977dadf3d8a

b02ba0b2a15d4673bb8757aec0d5426039b053ae

ea195b4a6303a794024f943b780a7bcc53e4e237

5bb123241e708622c749354f6bf0aa974b50a85a

a4e04c590badc8453e5c023b019497d0743706af

f4dee9d5bf57d506aecb781f920e23df4addef42

f146fd3f2e73e8493bc5f84a4a466b003336d54c

b4b0ee6e8b050c9308981a99a37a360f528f2be5

58b192f6b1a3047211075e3c421b3a911a57de7e

b792255bf814cc17ae9e485c8d241c98b1d2002c

61500d8c6b3f59a11fc45ed718fb3fa6458cc899

7540b3eaafb691d49aa2deb860038d4a74e48880

827eb25c94b5b9f7a560a90243a37f1084640e09

8b6bea72535bd51d08827a318f94dc9f600223fd

bb1fe9af77fd15c3c364222fd2ab0ca328a99a77

ff7566c450bdaafb02902e9f29f9bf544745ff52

0d22de8e31322991a9a7aa9325369cb218f2f978

8215604b5b223b529a78b2c09edb188426349a10

9d0c697862f16692d45bd4d873767d359ee37da3

5d32b522d3bcb98de1c280f1c101f95276f874f1

d9b7de23e27d7a130b28eaa753d6b1357f57119a

0aabdfad36c1ff4404374702e6ab18adcebad495

58e9e2f1546fa2764e19fb04d09762a9bcdd64ba

3747311bdc31fd84c228deac21055ad00dae9913

f11a0bdc939250493e1ca770599636aa5536325a

3fed056166be823c8c500bb5f5c0851c1267ec2c

f6c00d55c772601ab47f9d030f86092f3869cf22

d27f36404e1605d766d9e933834e35a5081a3a84

a35c2950c5227b94158b2cbff847648f3d62213a

caae132d30cb2a60799c04fe7444c95b78f383d6

abef532eb5283b45a488047af14b8ec3b430fca3

50931c16d015399b88a95a9a9d84639059b52ab1

7b8b12110dfa170e11bd641b207cd378b2b710c6

2b76dd6614d4642eec90a01aea94139eecede9fb

51d65c63671a2be351eae2c3638e468ec5122bd7

8350634c78402b3b962d7022f5228e2d43c729b9

The breach with reference number d9b7de23e27d7a130b28eaa753d6b1357f57119a was initially closed on July 1, 2021 with a closure letter. However, it appears from the letter that the Norwegian Data Protection Authority – typically if new information or complaints emerge in the case, or if the Norwegian Data Protection Authority receives new notifications about breaches of personal data security from the Family Court – will be able to reopen the case or allow it to be included in the assessment of any future breaches – or complaints. The breach in question is therefore also covered by this decision.

On 1 October 2020, the Danish Data Protection Authority started a case of its own motion against the Family Court, when the Danish Data Protection Authority was able to ascertain that the Family Court had notified 158 breaches of personal data security up to 27 September 2020, and that 130 of these notifications related to the accidental disclosure of personal data. The Danish Data Protection Authority made a decision in the case on 4 March 2021. The Data Protection Authority found, among other things, that the Family Court had not sufficiently ensured that the employees had taken the necessary care when processing citizens' personal data, including protected name and address information.

It was the Danish Data Protection Authority's assessment that the human errors could have been avoided by observing the necessary care on the part of the employees, just as the additional control carried out by another case manager was obviously not sufficiently effective. The Danish Data Protection Authority also stated that the Family Court should at the same time introduce effective technical control measures when sending case processing documents via electronic mail, so that these documents were not mistakenly sent to unauthorized persons.

The Danish Data Protection Authority found, on the basis of the above, that there was a basis for expressing serious criticism that the Family Court's processing of personal data had not taken place in accordance with the rules in the Data Protection Regulation, Article 32, subsection 1.

1. Decision

After a review of the case, the Data Protection Authority finds that there are grounds for expressing serious criticism that the Family Court's processing of personal data has not taken place in accordance with the rules in the data protection regulation[1] article 32, subsection 1.

At the same time, the Data Protection Authority finds that there is a basis for notifying the Family Court of an injunction to carry out a renewed risk assessment, based on the breaches referred to in this decision, in addition, on the basis of the risk assessment, necessary organizational or technical measures must be established. If the Family Court assesses that the risk to the rights and freedoms of the registered persons is high, the order also contains that the Family Court must draw up a consequence analysis, cf. Article 35 of the Data Protection Regulation.

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 6 January 2023. The Danish Data Protection Authority must request, by the same date, to receive confirmation that the order has been complied with and which changes to the technical and organizational measures have been implemented.

According to the Data Protection Act[2] § 41, subsection 2, no. 5, anyone who fails to comply with an order issued by the Danish Data Protection Authority pursuant to Article 58, subsection of the Data Protection Regulation shall be punished with a fine or imprisonment for up to 6 months. 2, letter d.

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

2. Case presentation

The breaches at issue in the case relate to the disclosure of protected addresses, protected names, telephone numbers, e-mail addresses, information about where the children go to school or institution, place of residence of one party, including names of shelters, first name and job title of the manager of a shelter , city or municipality, which could potentially reveal the party's whereabouts to the unauthorized recipient.

In most cases, the information has been passed on to the other party in the cases, which the persons have had name and address protection to avoid having to get the information, e.g. due to concerns about child abduction, violence, etc. or because the party does not want contact via email or telephone with the other party, who may also has a restraining order. In some cases, one parent has also been given a new name to hide from the other parent.

The information has been passed on in connection with responding to document access requests, sending decisions,

information letters and party hearings. The disclosures are mainly due to human error in the form of the case handlers not paying attention to the information and thereby not anonymizing it.

The Family Court has informed the case that, in the specific case, the Family Court assesses which measures the Family Court must offer the registered person(s) to remedy unwanted consequences of unauthorized disclosure of name and address information. Such measures can be advice and guidance on contacting the police if necessary, the possibility of seeking compensation for e.g. moving costs or guidance on making a name change.

As a starting point, the case manager will try to make quick contact with the person or persons involved to inform them about the data breach. This gives the citizen the best conditions to prevent any consequences. In this connection, the case manager will advise that the citizen has the opportunity to contact the Family Court's data protection adviser if the citizen wants further guidance or if special measures are needed.

In this connection, the Family Court has stated that in some situations the case manager will also make contact with the person who has received the information unjustifiably, if this is deemed appropriate. This may, for example, be the case if the recipient is a municipality, another authority or a lawyer who can be expected to help delete the information.

In the area of parental responsibility, where the Family Court can find that data breaches most frequently occur, where name and address protection is included, there is no catalog of measures. This will depend on a specific assessment in the case in question and will typically take place in collaboration with the Family Court's data protection adviser and the central legal unit.

Regarding the cause of the breaches of personal data security, where information about protected name and address has been inadvertently passed on, the Family Court has stated that the Family Court processes thousands of cases each year. In 2020, the Family Court ruled in 194,976 cases, including cases where protected names and addresses are included. Each case often contains a number of communication channels between citizens, other authorities or doctors and the Family Court.

In this connection, the Family Court has stated that the Family Court therefore has a strong focus on avoiding accidental disclosure of personal data, and that the Family Court continuously works to improve security. However, the Family Court has established that human errors can occur when employees perform their work, and that these errors can unfortunately lead to breaches of personal data security, where protected names and addresses are inadvertently passed on.

In divorce cases where a protected name or address is included, the Family Court has stated that they use the designations "your spouse", "mother", "father" and "child/children" instead of the names of the parties.

The Family Court has stated that when documents are accessed and uploaded to minretssag.dk, all documents are reviewed manually, and there is a procedure for the documents to be reviewed by two employees to ensure that, among other things, protected names and addresses do not appear in the documents and thus are passed on unintentionally.

As far as cases in the area of parental responsibility are concerned, the Family Court has stated that there are always disputes between the parties. There is therefore a greater risk of a data breach than in cases where only one citizen or addressee is involved. As a rule, there are submissions from at least two parties in each case, and the parties' submissions are sent as a starting point in a party hearing with the other party.

The Family Court has stated that when the party/parties have protected name and address, this is always clearly stated in the title of the case. In addition, the Family Court asks the parties to state whether, despite name and address protection, the Family Court may pass on the information to the other party, e.g. because the person concerned is already familiar with the information.

In addition, the Family Court has stated that the parties in the authority's cases are generally free to submit material to the extent and of the nature that the party deems relevant and has the opportunity to do so. Cases can therefore consist of a wide range of composite material. Anonymization will therefore never be possible solely through a purely technical solution using e.g. 'search-replace' functions or similar. According to the Family Court, there will therefore always be a certain risk of human error.

In some case types, manual entry/reporting is used, which also creates a risk of human error.

When asked what the Family Court has concretely done to reduce the number of accidental disclosures since the Data Protection Authority's decision against the Family Court of 4 March 2021, the Family Court has stated that they have appointed 27 GDPR ambassadors to support the work with data protection throughout the organization . The ambassadors participate in network meetings where data protection is discussed and where they are taught the data protection legal rules. They bring this knowledge to management and colleagues in the offices where the ambassadors are assigned.

The visibility of the GDPR ambassadors in the organization means that there has been an increased focus on data protection.

The Family Court has also stated that it is a fixed point at deputy director, head of office and unit meetings in the operational area to state and draw attention to the caution surrounding the processing of personal data. For use in these meetings, approx. every 14 days, management reporting to the business about breaches in the respective deputy director's area.

In addition, the Family Court has stated that in the area of family law they have changed their letterheads, so that the address is not automatically inserted. Only to the extent that the citizen does not receive digital mail, the case manager will have to find the address and put it in the letter.

In relation to cases relating to the area of parental responsibility, the Family Court has stated – with reference to the Danish Data Protection Authority's decision of 4 March 2021 – that resources have been set aside to help with anonymisation. Case handlers in the area of parental responsibility have the option of asking a team of student assistants to review the case and help with the concrete anonymisation. In this way, the Family Court wants to ensure that the procedure that there must be two case managers reviewing the case is not relaxed, due to busyness or lack of time resources.

Furthermore, the Family Court has stated that in order to ensure attention to special, concrete information of relevance in relation to data protection in the event of a upcoming document inspection, party hearing or case processing in general, notes are made on the cases in the Family Court's case processing system. This is done to ensure attention is paid to protection considerations when a case changes case manager and/or unit. The employees are instructed in connection with onboarding to always review case-level notes in connection with the processing of a case. It appears, among other things, of the visitation criteria, when a note must be placed on the case with special points of attention.

The Family Court has claimed that they are aware of continuously improving their proceedings and guidance in this regard. This means that if, in connection with a specific data breach, the Family Court discovers or assesses that the specific breach could have been avoided by another procedure, the Family Court incorporates the lessons learned from the specific error into their general work processes as soon as possible.

The Family Court has stated that the Family Court generally emphasizes to the case handlers that they must incorporate various practical routines in connection with the case handling. It could be, for example, not to have several case windows open at the same time when mail merges and subsequently sent, thereby minimizing the possibility of a technical merge error. It could also be to incorporate routines to always double-check and compare names and addresses on the letters with the party information in the case processing system before sending.

It appears from the Family Court's statement that in specific situations with technical challenges or system errors, the Family Court is aware of informing all employees of which specific, temporary instructions they must follow to remedy the specific problem. It can, for example, be due to an outcome of the CPR subscription. In that situation, instructions may be given to

always re-examine the parties in F2 for a period of time, before the case manager begins or continues a case, in order to ensure that the parties' information is updated with the latest information from the CPR, including information about names and address protection.

In addition, the Family Court has stated that relevant information is communicated via several channels, including the common intranet, concrete follow-up emails from function managers and by speaking at departmental meetings and/or meetings in specific teams. A specific ad-hoc instruction will also be written in Children and Parental Responsibility's ongoing visitation instructions. In this way, it is ensured that the precautions are observed at an early stage in the handling of the cases and before the case is transferred to a specific case manager.

The Family Court has also stated that data security is included as a theme in MUS and quarterly meetings, where the employee's focus on data security can be discussed with a function manager. In this way, the general focus on data security is maintained.

In addition, the Family Court has stated that data security is an important element in the reception and training of new employees. This is done by notification in the specific department already from the start of employment. New employees must also take a series of courses and tests on data and IT security in the Campus early in their employment and participate in general onboarding presentations from the data protection advisor and HR. In this connection, the Family Court has stated that in the past year and at the latest in May 2021, the Family Court has had a very large expansion of its staff in the area of parental responsibility.

Furthermore, the Family Court has stated that, despite a strong focus on data security in both on-boarding and concrete training, it can hardly be ruled out that the increase in productivity brought about by the increased recruitment is also reflected in the number of data breaches. In this context, the Family Court has noted that since 1 January 2020 the Family Court has increased the number of full-time employees by approx. 380.

In addition, the Family Court has stated that on 9 November 2021 the executive board decided on a concept for systematic follow-up of all data breaches, so that the focus is increased on reducing the number of data breaches and at the same time ensuring that the right measures are implemented so that similar breaches do not happen again. The concept means that all layers of management become aware of their role and responsibility in the process, and that handling and mitigating actions are monitored by the executive board. This will give the Family Court an increased focus on risks to the rights and freedoms of

the registered and thus an increased focus on a risk-based approach to data protection in the organisation.

In this connection, the Family Court has stated that, with the concept, it will be a requirement going forward that GDPR ambassadors and functional managers document decisions on mitigating measures in connection with each breach of personal data security. Mitigating measures – and any decisions not to implement mitigating measures – must be approved by heads of offices and deputy directors. Deputy directors report to the executive board, which approves the sections' work with data protection. On the basis of the reports, the executive board announces general data protection law topics that the organization must work with. The concept will eventually be expanded to also deal with the other requirements in the data protection regulation as well as tasks within information security. The expansion will take place in line with the implementation of the Family Court's re-implementation plan.

The Family Court has also stated that, in connection with the processing of adoption and guardianship cases, the Family Court is considering having the anonymization task supported by the system, so that it will be easier to search for and hide information that must be anonymized.

In connection with cases of separation and divorce, the Family Court is also investigating whether it is possible that any children are not created as parties to the case in the Family Court's case processing system, in order to avoid possible accidental disclosure when the wrong recipient is chosen in the case.

In conclusion, the Family Court has stated that, in general, GDPR ambassadors in the individual departments regularly prepare and carry out awareness events as needed and in agreement with the management, as part of their task of creating continuous awareness of data security. The effort will be expanded further in the future.

3. Reason for the Data Protection Authority's decision

It follows from the data protection regulation article 32, subsection 1, 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 severity for the rights and freedoms of natural persons, must implement appropriate technical and organizational measures to ensure a level of security appropriate to these risks.

It also follows from the regulation's article 32, subsection 1, letter d, that the data controller, depending on what is relevant, i.a. must implement a procedure for regular testing, assessment and evaluation of the effectiveness of the technical and organizational measures to ensure processing security.

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 for adequate security will normally entail that the data controller ensures that information about registered persons, including particularly confidential and sensitive information, does not come to the knowledge of unauthorized persons, that appropriate quality control of content should be carried out in forwarded documents with a view to avoiding disclosure of personal data to unauthorized persons, and that the handling of confidential and sensitive personal data places greater demands on employees' diligence in connection with the transmission of personal data, including ensuring that the correct information is sent to the correct recipient.

The Norwegian Data Protection Authority can ascertain that the Family Court – following the Norwegian Authority's decision of 4 March 2021 – has implemented significant organizational measures to avoid accidental disclosure of protected name and address information. However, the Danish Data Protection Authority is of the opinion that new and repeated breaches of personal data security or incidents that must be entered on the list required by the data protection regulation's article 33, subsection 5, should make the data controller reflect on risk assessments already made. Fracture types that are attributable to personal errors or isolated episodes should - if repeated - give rise to the introduction of additional effective control measures or technical support that minimizes the now known and actualized risks.

Examples of such measures can be, information minimization such that the address is only used in situations where it is required for the decision or necessary for sending by physical post, blocking in the ESDH system of sending information about addresses, other than to the person whose address it is, or it could be, the introduction of an actual Data Leak Prevention (DLP) system.

The Danish Data Protection Authority finds that the Family Court - by having ascertained and reported several similar breaches of personal data security, without having reconsidered the existing measures with a view to preventing future breaches of the same type - has not taken appropriate organizational and technical measures to ensure a level of security , which matches the risks involved in the Family Court's processing of personal data, cf. the data protection regulation, article 32, subsection 1. The Danish Data Protection Authority has placed particular emphasis on the fact that the Family Court has not had sufficient procedures for regular verification, assessment and evaluation of the effectiveness of the measures already established.

After a review of the case, the Danish Data Protection Authority finds that there are grounds for expressing serious criticism

that the Family Court's processing of personal data has not taken place in accordance with the rules in the Data Protection Regulation, Article 32, subsection 1.

When choosing to react in a stricter direction, the Danish Data Protection Authority has emphasized the fact that it can be associated with major consequences for the data subjects when their protected address or other place of residence, such as e.g. the name of a shelter, is inadvertently passed on to the person they are trying to hide from.

At the same time, the Data Protection Authority finds that there is a basis for notifying the Family Court of an injunction to carry out a renewed risk assessment, based on the breaches referred to in this decision, in addition, on the basis of the risk assessment, necessary organizational or technical measures must be established. If the Family Court assesses that the risk to the rights and freedoms of the registered persons is high, the order also contains that the Family Court must draw up a consequence analysis, cf. Article 35 of the Data Protection Regulation.

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 6 January 2023. The Danish Data Protection Authority must request, by the same date, to receive confirmation that the order has been complied with and which changes to the technical and organizational measures have been implemented.

According to the Data Protection Act[3] Section 41, subsection 2, no. 5, anyone who fails to comply with an order issued by the Danish Data Protection Authority pursuant to Article 58, subsection of the Data Protection Regulation shall be punished with a fine or imprisonment for up to 6 months. 2, 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] Act No. 502 of 23 May 2018 on supplementary provisions to the regulation on the protection of natural persons in connection with the processing of personal data and on the free exchange of such information (the Data Protection Act).

[3] Act No. 502 of 23 May 2018 on supplementary provisions to the regulation on the protection of natural persons in connection with the processing of personal data and on the free exchange of such information (the Data Protection Act).