Reports of breaches of personal data security

Date: 04-03-2021

Decision

Following a review of the Authority's cases concerning reports of breaches of personal data security, the Danish Data Protection Agency found that the Family Court has until 27 September 2020 reported 158 breaches of personal data security to the Authority in accordance with Article 33 of the Data Protection Regulation.

Journal number: 2020-432-0037

Summary

The Danish Data Protection Agency has reviewed the notifications in question to see if there is a coincidence in the reasons for the notifications, and if so, how cases of a similar nature can be avoided in the future. The Danish Data Protection Agency has therefore initiated a case of its own motion against the Family Court.

On the basis of a closer examination of the notifications received about breaches of personal data security, it was the Data Inspectorate's assessment that 130 out of 158 notifications concerned unintentional disclosure of personal data.

The Danish Data Protection Agency must initially state that the Personal Data Act per. 25 May 2018 has been repealed and replaced by the Data Protection Regulation and the Data Protection Act. This decision has therefore been taken in accordance with the current rules. As the breaches of personal data security have included periods, even before the Data Protection Regulation applied, the Danish Data Protection Agency has included this in determining the sanction.

The Danish Data Protection Agency must further note that the Family Court is organizationally based on the former “State Administration” and before this the “State Administrations” and the Family Court have thus, with the change in April 2019, taken over a large number of the already implemented IT systems.

Decision

After a review of the case, the Danish Data Protection Agency 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 Article 32 (1) of the Data Protection Regulation. 1.

Furthermore, the Danish Data Protection Agency finds that there are grounds for expressing serious criticism that the Family Court does not, in accordance with Article 28 (1) of the Data Protection Ordinance, 3 has complied with the requirement for a

written data processor agreement with the data processor CBRAIN A / S and that no written data processor instructions had been prepared for the data processor agreement with Visma Consulting A / S.

Overall, the Danish Data Protection Agency expresses serious criticism of the Family Court's violations of the Data Protection Ordinance.

Below is a more detailed review of the case and a justification for the Danish Data Protection Agency's decision.

2. The Danish Data Protection Agency has asked the Family Court for an opinion

Of the 158 reported processed reports from the Family Court, 130 were about unintentional disclosure of personal data, which is why the Danish Data Protection Agency decided to take up a case of its own motion, and in this connection requested the Family Court for an opinion in the case.

2.1. Statement of reports of breaches of personal data security

The Danish Data Protection Agency initially asked the Family Court to submit a statement of all breaches of personal data security regarding unintentional transfer of personal data to the Family Court in the period from 25 May 2018 to 27 September 2020, containing the elements that follow from Article 33 (1) of the Regulation. 5. Among other things, the Danish Data Protection Agency asked the Family Court to state what proportion of the detected security breaches - where personal information has been inadvertently passed on as a result of human / manual errors - constituted the Family Court's total outward communication with e.g. citizens, authorities, etc.

2.2. The Family Court's risk and impact analysis

The Danish Data Protection Agency requested the Family Court - in cases where outward communication takes place with e.g. citizens, authorities, etc., in connection with case processing - to account for the Family Court's considerations on the security and data protection law conditions and the risk of unintentional disclosure of personal data that were during the processing and the consequences that unintentional disclosure of personal data could have for the data subjects, especially in cases where information about protected names and addresses was passed on to another party in a conflict-ridden relationship.

2.3. The family court's technical and organizational measures

The Family Court was further requested to state whether special technical and organizational security measures have been taken, in order to ensure that information on protected names and addresses does not come to the attention of unauthorized persons and to forward all given instructions (with date of preparation) to the Family Court. employees regarding the handling

of personal data in connection with the transmission of information to e.g. citizens, authorities, etc.

2.4. Manual treatment or human error

As it has emerged from the Family Court's notifications to the Danish Data Protection Agency that in connection with case processing there has been unintentional transfer of personal data as a result of manual processing / human error, the Data Inspectorate asked the Family Court to state which relevant organizational and technical security measures were established prior to the letter date. , that personal information does not come to the attention of unauthorized persons in the event of unintentional disclosure and what technical and organizational measures the Family Court has implemented or intends to implement in order to avoid unintentional disclosures in the future.

2.5. Self-service solutions

In connection with the review of the reported breaches concerning unintentional disclosure of personal data, the Danish Data Protection Agency has found that a number of cases concerned unintentional disclosure of personal data in connection with the use of one or more of the Family Court's self-service solutions.

The Danish Data Protection Agency has therefore asked the Family Court to account for the specific circumstances that have led to the disclosure of personal information - including information about protected names and addresses - in connection with citizens' use of 5 self-service solutions performed by data processors Charlie Tango A / S (hereinafter Charlie Tango), CBRAIN A / S Hereafter CBRAIN) and Ditmer A / S (Hereafter Ditmer). The Family Court has also been asked to account for the relevant technical and organizational security measures taken by the Family Court and the relevant data processors prior to the breach and which have been implemented to deal with the breach and to stop the breach.

The Danish Data Protection Agency has also asked the Family Court to explain whether the individual data processors, in the Family Court's opinion, have violated the data processor agreements and instructions entered into and to submit the relevant data processor agreements.

2.6. The Family Court's guidelines for anonymisation

In connection with the review of a reported breach of personal data security, the Danish Data Protection Agency found that the Family Court had attached a document that was not sufficiently anonymised, which the Danish Data Protection Agency informed the Family Court about.

The Danish Data Protection Agency has asked the Family Court to describe the procedure for anonymisation that the Family

Court used until the Danish Data Protection Agency drew attention to the error of submitting any procedures for anonymisation that were in force before this and any subsequent corrected procedures.

3. The Family Court's information on the case

The Family Court has on 15 October 2020 sent an introductory statement, which on 2 November 2020 was supplemented with further information. Furthermore, the Family Court on 9 November 2020 sent a statement, related to the Family Court's self-service solutions.

3.1. Statement of breaches of personal data security

In the statement of breaches of personal data security, the Family Court has stated the number of cases in which personal information has been unintentionally passed on to 134. Of these breaches, 34 are cases involving persons with protected names and addresses. In the vast majority, these are human errors and in 12 cases the cause is stated as a technical error, of which 6 can be attributed to errors in letter merging.

In addition to ordinary personal information such as name and address, these include social security numbers, health information, ethnicity, significant social issues, economic conditions, religious and philosophical beliefs and sexual orientation.

In the 34 cases where there have been protected names and addresses, the information has in the vast majority of cases been passed on to another party in the case and in some cases to professionals, such as doctors, lawyers, municipalities or private companies.

3.2. The Family Court's considerations on risks

In the period from May 2018 to September 2020, the Family Court processed 421,665 decisions and processed 13,558 requests for access to documents, which is why the 134 breaches of personal data security constitute a very small part of the Family Court's total exchanges of personal information.

Nevertheless, the Family Court has an important task in continuously focusing on citizens' data security and follows the Danish Data Protection Agency's guidelines for dealing with breaches of personal data security. Therefore, the Family Court has worked with an increased level of awareness among employees and managers and on better training of employees with a focus on information security and data protection. Against this background, the Family Court expects an increase in reported breaches of personal data security.

The Family Court builds organizationally on the former State Administration and the work with implementation, data protection

and information security has historically not been sufficiently prioritized, which has left a significant organizational and technical debt and a general low maturity within the 2 areas.

In November 2019, the Family Court began the preparation of risk assessments and impact assessments that are anchored in risk matrices based on the COSO framework. In May 2020, the Executive Board approved a 2-year implementation plan in the field of data protection and information security. The recognition of the previously insufficient focus on the two areas has led to the Executive Board adding additional resources, including a dedicated project manager. In the autumn of 2020, the Family Court has begun to identify the need for additional resources for the area.

3.3. The Family Court's considerations on consequences

The Family Court handles many cases where the parties want a protected name and address. The Family Court has learned that it is of crucial importance that there is a clarification as to whether the name and address protection is valid. Therefore, the Family Court's case processing always begins with a clarification of whether the case is protected and whether this protection is applicable to the other parties to the case. In cases where name and address protection between the parties must be maintained, the Family Court makes a special effort to ensure the confidentiality of this between the parties and the Family Court's employees are fully aware of the far-reaching consequences it may have for those involved in the event of unintentional disclosure. of personal data. These major consequences are contained in the Family Court's risk assessments and willingness to take risks in the development of new technical solutions and organizational processes and workflows.

3.4. Special measures relating to name and address protection

At the Family Court, there are always 2 caseworkers who review the material before passing it on. In cases where name and address protection must be maintained between the parties, the Family Court makes a special effort to ensure confidentiality, e.g. through exemption and anonymization. A note for anonymisation and pseudonymisation has been prepared for this purpose in 2020. All files are indicated with the text "Protected name and address *" to reduce the likelihood of errors occurring, especially in case of a change of caseworker.

Part of the training of employees is to ensure rapid notification of the data subjects in order to reduce the negative consequences for the data subjects in the event of a breach of personal data security.

Since 2019, the Family Court has been working to gather the task of sending case files and personal data to the court to a specialized team to reduce the likelihood of errors.

As a technical measure, the Family Court has planned to develop a delayed sending of documents from the Family Court's ESDH system, which will mean that employees have the opportunity to withdraw correspondence within a pre-defined time period. As the Family Court's IT operations are to be transferred to Statens IT at the end of 2020, this solution is expected to be operational in the second quarter of 2021.

In collaboration with the National Board of Justice, a number of wrongful transfers have also been found to "minretssag.dk". In this area, a procedure has been developed that can make the information inaccessible to the parties and at the same time gather evidence for the unauthorized disclosure. It is thus possible to determine whether the information has actually been accessed and thus reduce the negative consequences for the data subjects' rights.

Protection of name and address information has been a separate point in the development of new technical solutions of the business, including encrypted video solution, for which instructions have also been prepared for employees to check whether the parties have protected name and address.

In connection with the established security breaches in some of the Family Court's self-service solutions in August 2020, the Family Court has reviewed all citizen-oriented self-service solutions in order to ensure that similar errors are not present. In those cases, the solutions have been closed and the breaches have been reported to the Danish Data Protection Agency.

It is the Family Court's clear intention that the self-service solutions must contain technical security measures that ensure that protected names and addresses are not passed on to unauthorized persons. In this connection, the Family Court has entered into an agreement with an external auditing company to review events and systems for all citizen-oriented IT solutions, as well as to provide input to a governance model that ensures a future effective, well-coordinated and robust structure for work with IT security, information security, ISO maturity and GDPR. The report has been sent to the Danish Data Protection Agency.

The Family Court has also sent appendices with instructions and instructions for the Family Court's employees regarding the handling of personal data in connection with the submission of material to citizens, authorities, etc.

3.5. Measures to address manual and human processing errors

On 5 May 2020, the Family Court has launched a major implementation plan that outlines a number of activities and focus areas for the next 2 years. A larger group of decentralized ambassadors has been appointed, who during 2021 will be trained in a wide range of key data protection law issues. The plan is also to focus on procedures and workflows, review data processor agreements, develop a new data protection policy under the Data Protection Regulation, and train decentralized

ambassadors.

In addition, the Family Court focuses on new procedures in portfolio management, audit of suppliers and contract follow-up.

3.6. The family court's self-service solutions

The Family Court gives citizens access to a total of 40 self-service solutions within, among other things, adoption, contributions, paternity, parental responsibility, complaints, divorce, guardianship and marriage for international couples. For 11 of these solutions - respectively visitation, residence, confirmation allowance, agreement application for child allowance, registration of shared residence, registration of termination of shared residence, application for change of custody of non-biological parents, change of residence and application to become an adopter - The Family Court has received inquiries about breaches of personal data security in connection with the unlawful disclosure of the names of citizens with name and address protection.

The data breaches are related to a technical deficiency due to a code error in a CPR call used in solutions offered by vendors Charlie Tango and CBRAIN.

3.7. Self-service solution for custody, residence and contact

On the basis of a citizen inquiry on 13 August 2020, the Family Court found an error in the self-service solution on 17 August 2020, where primarily parents, but also other applicants (eg grandparents) can apply for custody, residence and visitation. The integration between the self-service solution and the name and address protection registration in the CPR register did not work properly, which meant that the automatically generated receipts for submitted applications showed the full names of the children involved, even though they were registered with name and address protection in the CPR register. .

The solution was provided by Charlie Tango who is a data processor and subcontractor to Visma Consulting A / S (hereinafter Visma), with whom the then State Administration entered into a contract in 2018. There is a data processor agreement with Visma, but not a completed data processor instruction.

Initially, the subcontractor Charlie Tango announced that there was no problem in the solution, but found on the same day a significant problem in the integration to the CPR register.

3.8. Self-service solution for confirmation and clothing contributions

In January 2016, the then State Administration implemented a number of citizen-oriented self-service solutions, including for confirmation and clothing contributions. Prior to the implementation, the administration was aware that the system could not

separate the type of receipt response in the CPR call, which is why there was a risk that personal data for persons with name and address protection could be passed on incorrectly. Therefore, a message was stated in the self-service solution stating that sensitive personal data would be passed on to both child's parents, regardless of any name protection. If this was not desired, the citizen was directed to use an alternative manual form.

On 19 August 2020, the Family Court found a breach of personal data security in the Family Court's self-service solution, where parents can apply for confirmation and clothing contributions from the other parent. It was found that the Family Court had unjustifiably passed on information about the protected name of the child and the applicant parent to the other parent.

On 15 April 2020, the Family Court filed a change request with CBRAIN to rectify the error, but this was not initiated due to a "frozen period" leading up to the transition to Statens IT.

3.9. Self-service solution using DitmerFlex solutions

On 17 December 2017, a data processor agreement was entered into between the then State Administration and Ditmer on internal development DitmerFlex self-service solutions using Easy-ID login and digital mail. The systems were tested internally and put into operation with a subsequent hypercare period. On 7 September 2020, the Family Court became aware that 4 of the solutions - agreement application regarding contribution, registration of shared residence and registration of termination of shared residence and application to become an adopter - passed on protected names of citizens, knowing that the other party in the case, a copy was sent to the party's application / registration, in which no account was taken of any protected name of the party and the child referred to in the application / registration. The solutions were then closed.

It was decided that the solutions would only be implemented when the systems were prevented from disclosing protected names without consent and there was a solution to valid consent.

It is the Family Court's view that this is not a compromise of Ditmer's solution, but that the error has arisen in connection with the way the Family Court has used DitmerFlex.

3.10. Inquiries about affected self-service solutions

On 20 November 2020, the Family Court stated that for a total of 11 self-service solutions, the Family Court has received inquiries about unauthorized disclosure of names of citizens with name and address protection as a result of the error in the CPR call.

3.11. Notification to the data subjects

The Family Court has assessed that a total of 3493 citizens' personal data may have been unlawfully passed on and these persons have, with the assistance of the CPR office, been notified.

On that basis, the Family Court issued a notice on Friday 28.08.2020 about the breaches of personal data security to a total of approx. 3400 registered who were registered for digital mail.

The notifications are distributed over approx. 1,300 to parents who were covered by the data breach on the confirmation contribution solution, approx. 160 to young people over the age of 18, who were covered by the data breach on the confirmation contribution solution, approx. 1,800 to parents who were covered by the data breach on custody, residence and visitation solution and approx. 210 to young people over the age of 18, who were covered by the data breach on custody, residence and visitation solution.

In addition, the Family Court has sent 76 notifications by physical mail (such as Quickbrev), as the recipients were not registered / exempt from digital mail. Finally, 276 cases were selected for manual processing, as it was not clear from the available data base to what extent and to whom notification should be made. This has resulted in the sending of a further approx. 100 notification letters with digital mail.

The Family Court identified the directly affected data subjects as well as informed those who were deemed to be in the risk group. In the assessment, the Family Court has assumed that the recipient of the information about the protected name - in most cases the other parent - will most often have knowledge of the name of his children and his former partner in advance. In cases where, in connection with the registration of the name protection, no action has also been taken to change the name as part of identity protection, it is the Family Court's assessment that the disclosure of a protected name has not provided the other parent / applicant with information was familiar with.

Specifically, the Family Court has carried out a manual review of all the cases where, in addition to name protection, a name change has also been made. Following this, the Family Court has made an individual assessment of whether the data subjects in question are assessed to be directly affected by the data breach due to attempts at identity protection.

Based on this, the Family Court has estimated that there may be 11 directly affected, who in connection with the use of the self-service solution for application for custody, residence and visitation have been given the protected name of their child, and that there may be 5 directly affected, in connection with the use of the self-service solution for applying for confirmation / clothing allowance, their or their child's protected name has been passed on.

To the extent that these 16 persons have not already been in contact with the Family Court through our hotline or our data protection adviser, the Family Court has tried to contact them directly by telephone in order to provide advice and guidance. However, those directly affected have in any case received a letter of notification.

3.12. Data Processor Agreements and Data Processor Instructions

The Family Court has not entered into a data processor agreement with CBRAIN.

The Family Court has forwarded a contract entered into with Visma as far as the subcontractor Charlie Tango is concerned. Charlie Tango has performed services under a contract with Visma, but there are no formalized and completed data processor instructions, so it does not meet the conditions under Article 28 (1) of the Data Protection Regulation. 3. In the opinion of the Family Court, this is not a violation of the instructions entered into, but an error in setting up the test environment.

The Family Court has also submitted a data processor agreement with Ditmer. However, the agreement is not seen signed by Ditmer. It is not the Family Court's opinion that the data processor agreement has been violated, as there is no question of compromising Ditmer's solution. The error is due to the way the Family Court has used the solution.

3.13. Implementation of valid consent

As the practice regarding protected names and addresses, which the then State Administration had used since 2016, was considered to be in violation of good practice and current legislation, a change request was created at CBRAIN on 15 April 2020 to rectify the problem in connection with CPR call, but this was not initiated due to a "frozen period" leading up to the transition to Statens IT.

In connection with the Family Court's own development of form solutions in the program DitmerFlex, the Family Court has prepared and implemented a valid consent for 3 of these self-service solutions. The self-service solutions work in such a way that if the applicant / party states that they have protected their name in CPR, and that this may not be passed on, they are referred to apply / register the current application by filling in a PDF form, which is then sent to the Family Court. . The application / registration is then processed manually by the Family Court. The Family Court has stated that the consent will also be implemented in the Family Court PDF forms for the mentioned solutions. This work is in progress.

3.14. The Family Court's procedure for anonymisation

At the request of the Danish Data Protection Agency, the Family Court has submitted a procedure for anonymisation and pseudonymisation, dated 2 March 2020. The procedure has not been changed subsequently.

Of a reported breach of personal data security, the Danish Data Protection Agency's j.nr. 2020-442-8139, it appears that on 13 May 2020, an intentional transfer of personal data took place, as an insufficiently anonymised document was sent to a trade union instead of a hospital. The Family Court has stated that this was a human error.

4. Deloitte's report

At the request of the Family Court on 18 November 2020, the consulting firm Deloittes has prepared a report on business procedures and technical activities in connection with the self-service solutions' CPR call. The content of the report is in all material respects in accordance with the Family Court's statement. In the report, Deloitte has stated that:

The two reported data breaches relate to the systematic exposure of names of children and parents to the other parent, despite these persons' choice of and possible need for name and address protection to the other parent. The self-service solutions are citizen-oriented, and the exposure has been embedded in the solutions' automation, which is why the breaches are assessed by the Family Court's Data Protection Officer (DPO) as being of high risk, as the extent and consequences of the exposure may have been far-reaching.

Deloitte has further stated in connection with the investigation that the Family Court and CBRAIN in the implementation phase and in later updates of the self-service solution for confirmation contributions have not had a test frequency in the system, but that tests have been performed ad hoc. The test method has left a significant risk of human error in the test execution, which would not be present in, for example, automated tests. Deloitte has also stated that no tests were made of the effects of the changes in the production environment, but that a so-called "hypercare period" has been used instead, which has not been formalized in the form of clear definitions of which monitoring activities are to be carried out. performed and the frequency thereof.

On the basis of the investigations, Deloitte found that with regard to the solution for applying for contact, data in the test environment did not have sufficient similarity to the production environment, so the tests were not effective in identifying risks of exposure of protected data in connection with the solution's CPR. cold. Deloitte further concluded that another reported breach of personal data security in the contact solution - in the form that protected names have been visible in the contact solution - related to a similar technical deviation in the CPR call. The technical deviation in the CPR call has existed in the solution since its implementation in April 2019.

Based on the investigation, Deloittes has concluded that:

Based on the study, it is clear that all the identified data breaches in connection with CPR calls have existed in the solutions since their implementation. For confirmation contributions and parental responsibility, the implementation took place respectively. on 26 January 2016 and 1 April 2019. The defect has been documented to have a technical character, as the coding of the solutions did not succeed in separating resp. data display and receipt response, depending on whether the related citizens had name protection or not, why protected, personally sensitive data has been unlawfully passed on through step 4 of parental responsibility solutions and the process of automatic receipt writing in all four solutions. It is clear from the study that the Family Court's organization has historically been aware of the error and its consequences for the confirmation contribution solution, which is not the case with the parental responsibility solutions. The attention in the organization has been brought up in various forums internally on several occasions, primarily during the implementation of the solution, where a note on the problem was prepared, but also as late as the spring of 2020, where several function leaders and the responsible deputy director were made aware of the risk of fracture, however, without this leading to effective remedy. The organization has generally taken many good awareness initiatives in the field of information security, but it has been found that a lack of grounding in risk assessments, policies and procedures has contributed to the organization and management not being able to effectively communicate and remedy the breaches in the past.

Based on the report's observations, Deloitte has recommended that the Family Court prioritize a number of activities to remedy the observed risks and implement a strengthened framework for the organization's future work in the area of data management and information security.

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

The Danish Data Protection Agency has, through a review of the Family Court's submitted statement and accompanying appendices, as well as Deloitte's comprehensive review of the Family Court's business procedures and technical activities in connection with security breaches in 2 self-service solutions, gained insight into a number of Family Court proceedings. This includes guidelines for development, risk assessments, control of data processor agreements, the maturity of the technical solutions, operating and test environments, the staff's diligence in case processing, the established technical and organizational measures to ensure an appropriate level of security, and the family court's management knowledge of these matters.

The Family Court has stated in its statement that the Family Court is organizationally based on the former “State

Administration" and before this the "State Administrations" and the Family Court have thus with the change in April 2019 taken over a large number of the already implemented IT systems. The Family Court has in the statement maintained that the work of implementing data protection and information security has historically not been a sufficient priority area, which has left a significant organizational and technical debt, as well as a general low maturity within the two areas.

Based on the Family Court's own information and the study carried out by Deloitte, the Danish Data Protection Agency assumes that a number of self-service solutions for several years - for the self-service solution for confirmation contributions as far back as 2016 - have used faulty CPR calls, which has meant that the solutions have not been able to determine whether a citizen who used the solutions had protected his name and address, so that the citizen's personal data could unjustifiably be passed on to unauthorized persons in connection with the transmission of documents related to the citizen's case.

Furthermore, the Danish Data Protection Agency assumes that the Family Court has been aware of the erroneous CPR call, as the solution in 2016 introduced a message to users of the solution that the person's name would be passed on to others, regardless of any name protection.

On the basis of Deloitte's statement, the Danish Data Protection Agency also assumes that in the development of the systems, sufficient testing of the systems in question has not been carried out, partly because the test environment and production environment were not the same and no clear guidelines for testing and documentation of systems, including for critical systems such as CPR calls.

As a result of the Family Court's 134 reports of unintentional disclosure of personal data, of which in 34 cases information on persons with name and address protection, the Data Inspectorate is of the opinion that the Family Court - due to human errors attributable to employees - has not taken appropriate and adequate technical and organizational measures to ensure the continued confidentiality of this information.

Based on the Family Court's tasks, the Danish Data Protection Agency further assumes that the Family Court processes a lot of very sensitive and confidential information about a large part of the population and that sending this information to the wrong recipients can have a serious impact on the individual citizen's rights. safety, life and health.

5.1. Article 32 of the Data Protection Regulation

It follows from Article 32 (1) of the Data Protection Regulation 1, that the data controller must take appropriate technical and organizational measures to ensure a level of security that is appropriate to the risks involved in the data controller's processing

of personal data.

Thus, the data controller 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 put in place to protect the data subjects against these risks.

It is clear from Article 32 (1) of the Data Protection Regulation 1, that the data controller, taking into account the current technical level, the implementation costs and the nature, scope, coherence and purpose of the processing in question, as well as the risks of varying probability and seriousness of natural persons' rights and freedoms, shall implement appropriate technical and organizational measures to ensure a level of security appropriate to these risks.

The Danish Data Protection Agency is of the opinion that the requirement pursuant to Article 32 for appropriate security will normally mean that the data controller ensures that information about data subjects, including particularly sensitive information, does not come to the attention of unauthorized persons, that all probable error scenarios should be tested in development. of new software where personal data is processed, that appropriate quality control of content in submitted documents should be performed in order to avoid the transfer of personal data to unauthorized persons and that the handling of sensitive personal data places greater demands on employees' care in transmitting personal data, including ensuring that correct information is sent to the right recipient.

Furthermore, the Data Inspectorate is of the opinion that the Family Court's risk assessments do not adequately address the risk and consequence of employees sending information about registered persons to unauthorized recipients in the event of errors, misunderstandings or inattention, which can have serious consequences for the registered persons.

5.2. Technical measures test

The Danish Data Protection Agency finds that the Family Court, by not carrying out sufficient and regular testing of the developed self-service solutions before they were put into operation and by not ensuring that the test environments used were of a nature that made them suitable for performing this testing, has not complied with Article 32 (2) of the Data Protection Regulation 3, letter d.

It is the Data Inspectorate's opinion that test environments - compared with test strategies and clear guidelines - must have such a character that they give a true picture of how the tested systems will act in the production environment and that the testing must be regularly assessed and evaluated so that errors can be detected. before the systems are put into production.

Furthermore, the Danish Data Protection Agency is of the opinion that solutions that contain information of the nature

processed by the Family Court should not be designed to expose data as a starting point, but instead be designed to protect personal data and only expose it when relevant.

It is the Data Inspectorate's opinion that a data subject cannot, by consent, waive the protection of his rights, such as Article 32 of the Data Protection Regulation. In the self-service solutions where the Family Court has implemented what the Family Court calls a valid consent - and where they refer citizens who have protected name and address to fill in a form and send it to the Family Court instead of using the self-service solution - the Data Inspectorate finds it in addition, it is doubtful whether such information could be included in a consent that would meet the definition in Article 7 of the Data Protection Regulation.

5.3. Organizational measures

The Danish Data Protection Agency further finds that the Family Court has not sufficiently ensured that the employees have taken the necessary care when processing the citizens' personal information, including protected name and address information. As a result, the Family Court has not complied with Article 32 (1) of the Data Protection Ordinance. 1, letter b.

It is the Data Inspectorate's assessment that the human errors could have been avoided while observing the necessary care on the part of the employees, just as the extra checks carried out by another caseworker are obviously not sufficiently effective. At the same time, the Family Court should introduce effective technical control measures when sending case processing documents via electronic mail, so that these documents are not sent to unauthorized persons by mistake.

On the basis of the above, the Danish Data Protection Agency 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 Article 32 (1) of the Data Protection Regulation. 1.

5.4. Data Processor Agreements

Based on the Family Court's own explanation and submitted appendices, the Danish Data Protection Agency assumes that the Family Court has not entered into a contract with CBRAIN and that the contract entered into with Visma does not meet the formal conditions for data processor agreements, cf. Article 28 (1) of the Data Protection Ordinance. 3

On this basis, the Danish Data Protection Agency 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 Article 28 (1) of the Data Protection Regulation. 3.

The Danish Data Protection Agency is of the opinion that a contract between the data controller and his data processor must

contain all the elements necessary to determine the subject and duration of the processing, the nature and purpose of the processing, the type of personal data and the categories of data subjects, the data processor's obligations and responsibilities and obligations of data controllers in accordance with the rules laid down in Article 28 (2) of the Data Protection Regulation. 3.

5.5. Choice of sanction

When choosing a response, the Danish Data Protection Agency has emphasized that the Family Court processes a lot of very sensitive and confidential information about a large part of the population and that the disclosure of this information can have a serious impact on the individual citizen's rights and in extreme cases safety, life and health. .

At the same time, the Danish Data Protection Agency has emphasized that the violations - according to information - have been going on since 2016 and that the violations have been known among the organization's employees and middle managers for several years. In April 2020, function managers and the responsible deputy director were briefed on the issue, but planned mitigating measures were given low priority and therefore did not start. The Danish Data Protection Agency has also emphasized the high number of personal data that is processed, just as the data relates to persons, many of whom should enjoy special protection.

In addition, the Danish Data Protection Agency has emphasized that the Family Court has taken over the tasks of the former State Administration and thus a significant organizational and technical debt, as well as a general low maturity within the two areas that conditions the Family Court is working to rectify. The Danish Data Protection Agency has also emphasized that the Family Court in 2020 has launched a major implementation plan with a view to addressing manual and human processing errors.

5.6. Article 34 of the Data Protection Regulation

It follows from Article 34 (1) of the Regulation 1, that when a breach of personal data security is likely to involve a high risk to the rights and freedoms of natural persons, the data controller shall notify the data subject without undue delay of the breach of personal data security.

The Danish Data Protection Agency finds that the Family Court has acted in accordance with Article 34 (1) of the Data Protection Ordinance. 1.

In this connection, the Danish Data Protection Agency has emphasized that the Family Court, in collaboration with the data processors and the CPR register, has carried out a close review of all the persons affected by the breaches and, after specific

assessment, has informed those affected of the incidents.

5.7. Summary

On the basis of the above, the Danish Data Protection Agency 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 Article 32 (1) of the Data Protection Ordinance. 1.

Furthermore, the Danish Data Protection Agency finds that there are grounds for expressing serious criticism that the Family Court does not, in accordance with Article 28 (1) of the Data Protection Ordinance, 3 has complied with the requirement for a written data processor agreement with the data processor CBRAIN and that no written data processor instructions had been prepared for the data processor agreement with Visma.

Overall, the review gives rise to the Danish Data Protection Agency expressing serious criticism of the Family Court's violations of the Data Protection Ordinance.