Criticism of Gyldendal A/S for not meeting the requirement for adequate security

Date: 13-04-2023

Decision

Private companies

Criticism

Reported breach of personal data security

Access control

Notification of breach of personal data security

Treatment safety

Unauthorized access

The Danish Data Protection Authority criticizes Gyldendal A/S for not having arranged the URL sufficiently securely in Systime Screening, which provides access to a service used to screen students' skills at youth education institutions.

Journal number: 2021-431-0149

Summary

Gyldendal A/S provides the System Screening service, which is used by teachers at secondary education institutions to create tests. The purpose of the tests is to screen students for academic or skill strengths and weaknesses.

The tests are completed in a browser and accessed by clicking on a link sent via e-mail or by manually entering a URL. Access to answering the tests was only limited by the fact that users had to be logged in to a "My Account" on Systime. This meant that anyone logged in could complete the test if they entered a working link. Furthermore, the links that gave access to the tests consisted of shortened URLs. Specifically, a URL consisted of eight characters, with the randomized part being two characters. Only the creating teacher had access to the test results.

The simple URL and the access restriction set up on the tests meant that a student from one school – knowingly (e.g. for practice) or unknowingly (e.g. as a result of mistyping the URL) – could complete a test , which was created by a teacher from another school, through which teachers could gain - and did gain - unauthorized access to other than their own students' name, email and screening results.

Gyldendal A/S deliberately designed the solution in this way to ensure a high degree of flexibility, and the URL was shortened

according to the wishes of their customers, because they had system technical limitations in their IT setup.

Risk of incorrect entry of URL must be accommodated

The Danish Data Protection Authority established in the case that processing activities that can be accessed via URL must take place in a way that ensures the confidentiality of personal data. This places demands on the layout of the technical solutions, and it implies, among other things, that you have to make sure that students do not inadvertently share their personal data with third parties.

In the specific case, Gyldendal A/S' layout of the URL did not meet the requirement for adequate security in the GDPR. This was because the device did not take into account URL manipulation/change and wrong entry, which are commonly known sources of error that should be easily countered by the data processor, and that the purpose of the tests was clearly to process personal data worthy of protection.

The Danish Data Protection Authority also noted that the installation of a solution that impairs the rights of data subjects cannot be justified solely because the data processor's customers (the data controllers) have system technical limitations in their IT setup.

Decision

The Danish Data Protection Authority hereby returns to the case where, on 27 September 2021, based on reports from four data controllers about breaches of personal data security, the Danish Data Protection Authority chose to initiate a collective action against the data processor Gyldendal A/S.

1. Decision

After a review of the case, the Danish Data Protection Authority finds that there is a basis for expressing criticism that Gyldendal A/S processing of personal data has not taken place in accordance with the rules in the data protection regulation[1] article 32, subsection 1.

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

2. Case presentation

It appears from the case that Gyldendal A/S, including Systime, is a data processor for a total of 128 youth education institutions. Gyldendal A/S has offered the "System Screening" service since 2010. The service can be used by teachers to create tests (questions and problem solving) aimed at screening students. The purpose of the screening result is to provide an

indicative snapshot of the students' general or specific professional or skill strengths or challenges, including e.g. speech or speech blindness.

The test is accessed and answered via a link sent to the student's e-mail, or by the student manually entering the link in a browser. Before the test can be answered, the students must have created themselves as users of MinKonto in Systime and be logged in to this account. The result of the test is not forwarded to the student himself, but appears exclusively on the creating teacher's results module.

Gyldendal A/S has stated that students' affiliations are not validated in relation to their respective educational institutions. Systime Screening therefore does not know which educational institution a student is affiliated with. Systime Screening cannot therefore prevent a student from taking a test created by a teacher from another school. Gyldendal A/S has stated that this flexibility is a conscious choice, which, however, means that the tool can be used in inappropriate ways - and that the reported breaches apparently just happened through inappropriate use of Systime Screening.

The type example – which requires the breach of personal data security – consists of a teacher from school A creating a test that is inadvertently accessed and answered by an unauthorized student from school B. On this basis, teacher A gains unauthorized access to an arbitrary student from school B screening result, name and email. As stated, the invitation link is not set with an access barrier, including associated with a specific student. Anyone with access to the link can thus complete the test after logging into MyKonto in Systime Screening.

Gyldendal A/S has identified the following five typical scenarios for how this is supposed to happen:

A teacher from school A is not aware of the license conditions for the use of Systime Screening and has agreed with a teacher from school B that students at school B can take their tests with teacher A's access.

A teacher from school A creates and shares an invitation link in a publicly available document – e.g. a lesson plan. A student from school B finds this link by chance or by searching and wants to practice before the student himself has to be screened at his own school.

A student at school A has been screened by his teacher from school A. The student has friends who attend school B in the same year. The student suggests to his friends at school B to practice before they too have to be screened and sends them the invitation link. The classmates at school B therefore take teacher A's test.

A teacher at school A shares an invitation link by inserting it into the school's LMS system. The LMS system's editor has set up

rules for the use/display of certain characters in links, after which this editor changes or removes certain characters in the link. This may cause the link to no longer refer to a test created by a teacher from school A, but to a test created by a teacher from school B.

A teacher from school A shares a link by writing it up on a whiteboard, from where students have to type it into their browser's address bar. During the manual copying, one or more characters may be omitted or mistakenly perceived as another, so that the link the student accesses has become a link to a test created by a teacher at school B.

Gyldendal A/S has further stated that the links are generally very long, which is why they use a URL shortener that significantly shortens the URL. Gyldendal A/S states that they have shortened the links at the request of customers whose LMS systems do not allow long links.

Gyldendal A/S has stated that, on the basis of the inquiries about the breaches, a reassessment of the risks of using Systime Screening has been carried out, just as the correct use of the tool has been tightened towards the data controllers.

In this connection, it was assessed that the incidents most likely relate to the above-mentioned scenario 5. It is thus hypothesized that in the period just before the incidents, the aforementioned URL shortener used a number of specific characters, which are particularly suitable for confusion in connection with manual copying of links.

Based on the hypothesis, adjustments have been made to the URL shortener with a view to reducing the risk of scenario 5 (minimizing the risk of student typos). In this connection, Gyldendal A/S has stated that the short links before the adjustment were quite short (8 characters), with the randomized part filling 2 characters. After the adjustments, the short links are now a minimum of 12 characters, of which the randomized part is 3 characters. At the same time, a number of characters that are particularly suitable for confusion were excluded – e.g. zero and capital O, capital I and small L, etc.

Gyldendal A/S further states that students cannot - by changing the URL - access other people's tests. In all cases, only those who have access to the creating teacher's results module can gain insight into the personal data. It is not possible for them to change or delete the personal data.

It appears from the case that Gyldendal A/S can see tests created by teachers and the answers. Gyldendal A/S cannot see with whom the links have been shared, and therefore cannot provide information on the extent of the incident, including the number of affected registrants. It has therefore also not been investigated whether the affected personal data has been used.

Gyldendal A/S has stated that the potential consequences of a third party's unauthorized knowledge of a student's academic

ability may cause the affected students to be embarrassed.

Gyldendal A/S has stated about their prior measures that they have instructions and FAQs in the product and trading conditions on Systime's website.

Gyldendal A/S has attached a reference to their instructions for creating and handling tests. It appears from this under the subject field "Share a test with your students":

"Be aware:

that you may only share the link with students and colleagues at the school/institution where you are employed. The screenings must not be used in schools other than the one that has the license to do so.

that students may not access links to screenings that come from other schools, nor may students forward the link to others, as the recipient's results and personal data will appear in your results summary.

that you must not publish screening links on web pages or in documents to which anyone other than students or colleagues from your school/institution has access."

Gyldendal A/S has finally stated that the data controllers have been notified on 13 August 2021.

3. Reason for the Data Protection Authority's decision

Based on the information provided by Gyldendal A/S, the Danish Data Protection Authority assumes that teachers, when using Systime Screening, have had unauthorized access to students' screening results, including entered names and e-mails, which is why the Danish Data Protection Authority finds that there has been a breach of personal data security , cf. the data protection regulation, article 4, no. 12.

3.1. Article 32 of the Data Protection Regulation

It follows from the data protection regulation, article 32, subsection 1, that the data processor must take appropriate technical and organizational measures to ensure a level of security appropriate to the risks involved in the data processor's processing of personal data.

The data processor thus has a duty to identify the risks that the data processor'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 mean that in systems with a large number of confidential and protection-worthy information about a large number of users,

higher requirements must be placed on the care of the data processor in ensuring that there is no unauthorized access to personal data.

A service that clearly aims to process and evaluate personal data worthy of protection about professional ability places great demands on the data processor's design of their technical solution. Processing activities that can be accessed via a URL must take place in a way that ensures the necessary confidentiality, so that the data subjects do not inadvertently and without being aware of this pass on personal data to third parties who do not have a work-related or other legitimate need for access to the information.

It is the Danish Data Protection Authority's opinion that URL manipulation/change and incorrect entry is a type of error source which is common knowledge and should be easily countered by the data processor. Furthermore, the Danish Data Protection Authority is of the opinion that a shortened link consisting of 8 characters, where the randomized part takes up 2 characters, is generally not an expression of adequate protection, as the structure of the structure of the link provides a limited entropy and does not remedy the identifying error scenarios.

Furthermore, the Danish Data Protection Authority is of the opinion that a data processor must continuously carry out an assessment of the risks their system entails when processing personal data. System technical limitations in a data controller's IT setup cannot in themselves justify that there is no adequate protection of the data subjects' rights in the processing of personal data that is carried out.

Based on the above, the Danish Data Protection Authority finds that Gyldendal A/S - by not having implemented sufficient access barriers for access to answering the screening tests, including the entropy of the selected URL - has not taken appropriate organizational and technical measures to ensure a level of security that suits to the risks involved in the company's processing of personal data, cf. the data protection regulation's article 32, subsection 1.

After a review of the case, the Danish Data Protection Authority finds that there is a basis for expressing criticism that Gyldendal A/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 a response, the Danish Data Protection Authority has emphasized that Gyldendal A/S has not, in view of the screening test's clear purpose of processing personal data worthy of protection, arranged their URL in a sufficiently secure manner, and that the weakness in question is of a known nature.

The Danish Data Protection Authority has further emphasized that the conditions have been present for over 10 years, some of which, however, predate the application of the Data Protection Regulation and that the breach has affected a large number of students from potentially 128 youth education institutions.

The Danish Data Protection Authority has noted that Gyldendal A/S has carried out a reassessment of the risks when using Systime Screening, and that, based on this, adjustments have been made to the URL, so that the risk of incorrect entry is minimised. In addition, Gyldendal has informed the data controllers on 13 August 2021. In a further mitigating way, the Data Protection Authority has placed importance on Gyldendal A/S's cooperation in clarifying the case.

The Danish Data Protection Authority has also noted that Gyldendal A/S has prepared a guide aimed at the data controllers, which instructs how Systime Screening should be used appropriately and that the correct use of the tool has been reinforced towards the data controllers.

3.2. Summary

The Danish Data Protection Authority finds that there is a basis for expressing criticism that Gyldendal A/S processing of personal data has not taken place in accordance with the rules in the data protection regulation, article 32, subsection 1.

[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).