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

Date: 21-06-2022

Decision

Private companies

Serious 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 expresses serious criticism of Gyldendal A/S for not taking into account URL manipulation in the layout of the URL, which provides access to a service used to screen school students' skills.

Journal number: 2021-431-0149

Summary

Gyldendal A/S offers the Systime Screening service, which is used by teachers in schools 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.

The answers to the tests are not subject to any access restrictions. This means that anyone can complete the test if they – intentionally or accidentally – enter 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. These links could only be accessed by those who had access to the teachers' results module.

The simple URL and the lack of access restrictions on the tests meant that teachers could get - and did get - unauthorized access to students' tests. Access took place i.a. know that a student from one school completed a test created by a teacher from another school. In this way, teachers gained unauthorized access to students' names, e-mails and screening results.

Gyldendal A/S deliberately designed the solution in this way to ensure a high degree of flexibility. The URL was shortened according to the wishes of their customers, because the customers had system technical limitations in their IT setup.

Risk of URL manipulation must be addressed

The Danish Data Protection Authority ruled in the case that personal data that can be accessed via URL must be arranged in a way that ensures the confidentiality of the personal data. This entails ensuring that third parties do not potentially gain unauthorized access to the information.

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 layout did not take into account URL manipulation, which is common knowledge and should be easily accommodated, 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, on the basis of 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 Data Protection Authority finds that there are grounds for expressing serious 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 number of municipalities, including a total of 128 schools. Gyldendal A/S has offered the "System Screening" service since 2010. The service can be used by teachers in schools 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 academic or skill strengths or challenges, including e.g. speech or speech blindness. The test is answered by clicking on a link sent via e-mail or by manual entry. The answer is then done in a browser. 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 in relation to the matter that the affiliation of students is not validated in relation to their respective educational institutions. This means that any student, with the link in hand, can access the test. Gyldendal has stated that the great flexibility is a conscious choice, which, however, means that the tool can be used in "inappropriate ways". The type example – which requires the breach of personal data security – consists of a teacher from school A creating a test that is inadvertently taken and answered by an unauthorized student from school B. On this basis, teacher A gains unauthorized access to the screening result of an arbitrary student from school B , name and email. 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, which in practice e.g. can be done by sharing the link in a publicly available document. Another scenario could be that a student forwards it himself or enters it incorrectly due to a typo.

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 states that they have shortened the links "at the request of customers whose LMS systems do not allow long links." In addition, Gyldendal A/S describes how the URL was before the adjustment based on the specific incident: "The short links were quite short before the adjustment (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." This is intended to minimize the risk of students' typos. 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 scope of the incident, including the number of affected registrants. 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". In addition, it is stated that all teachers can hypothetically 'harvest' arbitrary students' personal data.

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. It has not been investigated whether the affected personal data has been exploited. Based on

inquiries about the specific incident in August 2021, Gyldendal A/S reassessed the risks of using Systime Screening. In addition, they reinforced the correct use of the host clothing towards the data controllers

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" that:

"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."

Finally, Gyldendal A/S informs 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 school 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, of 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 no unauthorized access to personal

data occurs.

A service that clearly aims to process and evaluate personal data worthy of protection on minors, including professional ability and derived health information, places greater 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 third parties do not potentially gain insight into and edit access to information where there is no business need.

The Danish Data Protection Authority is of the opinion that URL manipulation is a type of programming error source which is common knowledge and should be easily countered by the data processor. In addition, 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 there is both a fixed structure in the structure and an extremely limited entropy.

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 has 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 data subjects' rights.

Based on the above, the Danish Data Protection Authority finds that Gyldendal A/S – by not having implemented sufficient access barriers for access to and editing of 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 fits 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 are grounds for expressing serious 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 predate the application of the Data Protection Regulation and that the breach has affected a large number of registered minors from potentially 128 schools.

The Danish Data Protection Authority has noted that Gyldendal A/S has subsequently carried out adjustments to the URL, so

that the risk of incorrect entry and URL manipulation is minimised. In addition, Gyldendal has informed the data controllers on 13 August 2021. In a further mitigating way, the Data Protection Authority has emphasized Gyldendal A/S' cooperation in clarifying the matter.

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 is appropriately used. This has been tightened towards the data controllers. In addition, the Danish Data Protection Authority has noted that Gyldendal A/S has carried out a reassessment of the risks when using Systime Screening.

3.2. Summary

The Danish Data Protection Authority finds that there are grounds for expressing serious 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).