Serious criticism of Helsingør Municipality in Chromebook case

Date: 10-09-2021

Decision

The Data Protection Authority has decided the first in a series of cases involving the use of Google Chromebooks and G Suite for Education (now called Workspace) in primary school.

Journal number: 2020-431-0061.

Summary

The Danish Data Protection Agency's decision in the specific case of the use of Google Chromebooks in Helsingør Municipality states that the Folkeskole Act gives the municipalities the right to choose the IT equipment and programs to be used in the teaching.

It is the responsibility of the municipality as data controller to ensure that the IT equipment and programs are used in such a way that the data protection rules are complied with. In particular, that the treatments performed do not go beyond the purpose prescribed by the Folkeskole Act. The Danish Data Protection Agency mentions as an example of such a purpose disclosure, where information is used for marketing or profiling of services.

In the specific case, the municipality had not made the necessary assessments of the risk to the data subjects' rights.

The Data Protection Authority states in the decision that for parts of the user creation for the Chromebook and the use of G-Suite, it is necessary to configure the access to the applications and the way in which they work in order for these to be used legally.

As the municipality had not assessed this, the municipality also did not have documentation that the configuration had taken place in a way that suited the risks for the data subjects.

The Danish Data Protection Agency found that the missing assessments led to several breaches of the regulation.

The Danish Data Protection Agency issued an order to Helsingør Municipality to bring the processing of information in accordance with the regulation. If the municipality could not reduce the risk of the processing, the municipality was imposed a restriction which means that the municipality may not process the information in question after a given deadline.

In addition, the Authority expressed serious criticism of the municipality's treatments. The audit also gave the municipality of Helsingør a warning that the use of additional products for G-Suite could not be processed legally without an impact

assessment, where risks of the treatment were reduced to less than a high risk for the data subjects' rights and freedoms.

Decision

The Danish Data Protection Agency hereby returns to the case where Helsingør Municipality on 29 January 2020 reported a breach of personal data security to the Danish Data Protection Agency.

The review has the following reference number: ce0e5422ddfb3fefaa9f621cfa0f129127058500.

On the basis of several relatively uniform breaches by other data controllers, parts of the case information have taken place together and in parallel in these cases.

Decision

After a review of the case, the Danish Data Protection Agency finds that there are grounds for issuing an order to the Municipality of Elsinore to bring the processing using Chromebooks in accordance with the regulation, cf. Article 58 (1) of the Data Protection Regulation. 2, letter d. This must be done by the municipality of Elsinore before 1 November 2021, doing the following: Risk assessment of the treatments in Chromebooks and G-Suite, which reflects the flows of personal data the treatments entail. The risk assessment must partly address the necessary options for configuring the product and address the questions about the scope of the authority in the Primary and Lower Secondary School Act in relation to the use required of the pupils. If the risk to the data subjects and their liberties is assessed as being high, the order also includes the preparation of an impact assessment.

The Danish Data Protection Agency issues a warning to the municipality of Helsingør that the use of G-Suites 'supplementary programs without carrying out data protection law impact assessment will be contrary to the Data Protection Ordinance, unless it is proven by the now mandated assessment that the risk to data subjects' rights and freedoms is not high. . The warning is issued in accordance with Article 58 (2) of the Data Protection Regulation. 2, letter a.

If the assessments of the risk made by Helsingør Municipality show a high risk to the data subjects' rights and freedoms, and these risks have not been reduced to a level less than high before the order deadline expires on 1 November 2021, the Danish Data Protection Agency hereby announces a temporary limitation of the processing, so that processing involving a high risk of the data subjects' rights and freedoms, after this date, may not take place as long as the risk has not been reduced to a level lower than high. The processing restriction is notified in accordance with Article 58 (2) of the Data Protection Regulation. 2, letter f.

Failure to comply with an order or a temporary restriction may, unless a higher penalty is due, be punished by a fine or imprisonment for up to 6 months, cf. section 41 (1) of the Data Protection Act. 2, No. 4.

For the violations found, the Danish Data Protection Agency, in addition to the already chosen corrective measures, expresses serious criticism that the Municipality of Helsingør's processing of personal data has not been in accordance with the Data Protection Ordinance

Article 5, paragraph Article 5 (2) 1, letter c and letter f.,

Article 5, paragraph Article 6 (1) (a)

Article 32 (1), (1), (33) 1 and 35, para. 1.

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

2. Case presentation

On 29 January 2020, Helsingør Municipality reported a breach of personal data security to the Danish Data Protection Agency. It appears from the review and subsequent detailed statements that Helsingør Municipality has handed out Google Chromebooks to the municipality's school students for use in teaching in the municipality's primary schools. In connection with the handover, the municipality has set up access to the Google G-Suite for education (hereinafter G-suite), for which use a Google account must be used. For this school account, the student's full name has been used and thus been available for other of Google Inc. '(hereinafter Google) products, to which the created school accounts were passed on by Google - here under the program YouTube - which Helsingør Municipality was not aware of, just as it was not the intention. It further appears from the case that the students - if they used the program YouTube - automatically gained access to their school account and had their full name displayed in connection with their posting on this platform, unless the students had been assigned anonymous usernames by the municipality.

It appears from the case that Google - according to information since 2015 - has offered a software package called G-Suite. The program package is particularly aimed at teaching children and young people and is therefore considered suitable for teaching. The programs can be provided by a number of companies as a package solution, which can include a laptop, software package, installation and setup, as well as specially developed teaching materials. In order for students to access the G-Suite programs, they must have set up a school account with Google. The account can be created manually, but it is also possible to create school accounts by transferring first and last name, school and grade level from the schools' administrative

systems, however, so that students with protected name and address information could be anonymized by assigning the student an alias instead. for the student's name. Despite this, there have been several instances where students' full names have been listed instead of aliases.

Helsingør Municipality has - like a large number of the country's municipalities - acquired and handed out laptops with the installed software package based on their exercise of authority in accordance with the Folkeskole Act, which is why they have not considered it necessary to obtain guardians' consent to establish of students' school accounts with Google.

In 2019, Google changed the terms of use for G-Suite so that a number of additional products were perceived by the agreement entered into. These products included YouTube, G-mail, Blogger, Google+, etc. and Google states that the Terms of Use apply to all services provided by Google and its affiliates, including YouTube.

Google's provision for the use of G-Suite states that access to the system for children under the age of 13 requires parental commitment and for young people under the age of 18, access to the supplementary systems, including YouTube, also requires parental commitment.

G-Suite has a user administration module that allows you to choose which systems and additional systems the students should have access to. It is thus possible, by active action, to close off students' access to e.g. YouTube, G-Mail, etc ..

School students in Helsingør Municipality have with their school accounts gained access to the additional products and thus the opportunity to make posts and comment on other people's posts on, for example, YouTube. In this application, information about the name, school and class with which the student is created will be displayed in connection with the notice.

The Danish Data Protection Agency has received 2 complaints regarding Helsingør Municipality's processing of personal data in connection with the delivery of Chromebooks. Both complaints show that Helsingør Municipality, without the parents' knowledge and consent, has set up Google accounts for the students, with which the students have gained access to a number of Google's programs under G-suite, including G-mail and the additional product YouTube. The complaints further state that the students' full names are displayed using G-mail and that the parents do not have the opportunity to correct or anonymize this information, as only Helsingør Municipality has access to the user administration panel.

Furthermore, it appears that the students' full name, school and grade level appear on YouTube if the student has made or commented on posts.

The complainants further point out that the handed over computers have pasted the students 'login information, which is why

there is really no security against unauthorized access to the students' accounts.

3. Helsingør municipality information

Helsingør Municipality has stated in a consultation response to the Danish Data Protection Agency that the municipality has entered into a data processor with Google on the use of Chromebooks and the creation of school accounts that contain the students' name, school and grade level. The school profiles have been created with reference to the schools' exercise of authority in accordance with the Folkeskole Act, where they are legally obliged to teach IT. For this reason, the municipality has not obtained the parents' consent to the creation of accounts for the students. The municipality has further stated that for a school profile for G-suite, the student owns all the data.

When creating the students' school accounts, data is retrieved from the school administration system, but in connection with protected name information, a procedure is followed in which an alias is assigned instead of the student's full name. Helsingør Municipality has stated, however, that the municipality in several cases, has stated a student's full protected name instead of alias, whereby there has thus been a risk that the protected name could be the subject of publication.

In connection with changing Google's terms of use of the G-suite, a number of add-ons, including Youtube, were made available to school students through their school account. Helsingør Municipality has not been aware of this.

Helsingør Municipality has in a consultation response of 6 January 2020 confirmed that a parent in 2019 complained that his child - without his knowledge - had set up an account for YouTube, whereby the child's name could be published on Youtube. As it has not been the intention that the students should use other programs than the core programs in G-suite, Helsingør Municipality has not been aware that the use of the supplementary programs could result in the publication of the students' names on e.g. Youtube. For the same reason, Helsingør Municipality has not carried out a risk assessment, including for loss of confidentiality, for the treatment in question. In the same way, Helsingør Municipality has not implemented technical or organizational measures to ensure the data subjects' rights in connection with the use of social media using the established school account.

Helsingør Municipality has closed the access to Youtube via G-Suite and thus ensured that students will not be able to publish information about themselves in the future. The municipality states, however, that it is the student's parents' responsibility to delete the student's profile and possibly unwanted content on social media, as it can not be done via the municipality's user administration panel. The municipality has stated that the municipality has changed the publicly available information to only

include first name and school.

Helsingør Municipality has assessed that it was unlikely that the incident could entail a risk to the data subjects' rights and freedoms and therefore has not given rise to notification to the Danish Data Protection Agency. Helsingør Municipality has assumed that the information that was inadvertently shared with Youtube consists of ordinary personal information in the form of names, school and grade level, information which in the municipality's opinion in itself does not allow the person to be contacted directly or collected behavioral information. In addition, Helsingør Municipality has assumed that Youtube is owned by Google and that Google has not been given access to further information than what has already been given access to within the original G-suite agreement. The municipality has further assumed that the information in question is general information, where it is unlikely that this in itself can be misused for e.g. identity theft.

On 21 January 2020, Helsingør Municipality has notified all parents of the incident and the municipality has sharpened its attention to the settings in the user administration console for G-suite.

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

4.1 General

It follows from the Folkeskole Act § 2, paragraph. 1, that the municipal council is responsible for the primary and lower secondary school.

In addition, it follows from the compulsory school, from section 18, subsection 1 and section 19 of the same Act, that this includes the organization of teaching, including the choice of teaching and working methods, methods, teaching aids and substance selection, as well as the payment for this.

It is the Data Inspectorate's opinion that both choices about the use of IT in teaching and which brand and software to use fall within this scope.

The data protection rules are technology-neutral, and the Danish Data Protection Agency can only assess the circumstances that follow from the processing of personal data that is carried out, cf. Article 2 (1) of the Data Protection Regulation. 1.

This decision therefore only concerns the processing of personal data that takes place on the selected equipment and software, and whether these take place within the framework prescribed by the Data Protection Regulation and the Data Protection Act.

4.2 Use of Chromebooks and G-Suite

The rights of children and young people enjoy special protection in the data protection rules. It is the opinion of the Danish Data Protection Agency that this consideration is included in the assessment of which treatments can be carried out on the basis of the authority given by the Folkeskole Act to the individual municipality.

As the case is available to the Authority, and after a review of the submitted material, the data processor agreement with Google, as well as a review of the possibilities for configuration when creating users and configuration of settings in the applications, it is the Data Inspectorate's opinion that Helsingør Municipality, would have be able to supply Chromebooks and deploy G-Suite (the original core applications) for educational purposes, and process the required information in accordance with Article 6 (1) of the Data Protection Regulation. 1, letter e, this also applies to the creation of the individual student as a user of the system.

In this assessment, the Danish Data Protection Agency has placed special emphasis on the fact that the use of a Chroomebook, the basic creation of students in the system and the use of the part of G-Suite that make up the basic package can be configured so that there are no treatments that exceed it. The municipality has room for maneuver within the framework of the municipality's exercise of authority, in accordance with the provisions of the Folkeskole Act on the purpose of the folkeskole and the provision of teaching aids. The Danish Data Protection Agency has assumed that it appears from the data processor agreement and the possibilities for configuring the individual units that data can also be personal data managed so that this is not processed outside the EU / EEA, that the information about the individual user can be data minimized to an alias and that data including personal data created using the applications in G-Suite (the Core Programs) can be configured so that only the individual registered student and administrators authorized by the municipality will be able to access this data, including in particular that the information will not be used for marketing, neither directly as targeted to the individual student nor indirectly as part of a group (class, grade, school, etc.).

It is the Data Inspectorate's assessment that this configuration, especially in relation to some of the applications, will require that parts of the functionality be shut down. In addition, the Danish Data Protection Agency's assessment is that when using the product without this configuration, and with completely ordinary and expected use of the equipment, it will be possible to transfer personal data to services outside the EU / EEA. Such transfers will require compliance with the rules of Chapter 5 of the Data Protection Regulation.

It is a precondition that some documented choices have been made prior to commissioning, which in part ensures compliance

with the principles of Article 5 (1) of the Data Protection Regulation. 1, in this case especially letters c and f, partly ensures that it is assessed before commissioning. whether an impact assessment is to be carried out in accordance with Article 35 of the Data Protection Regulation. This assessment must also be used in order to be able to select the required level of security in accordance with Article 32.

The Data Inspectorate assumes - in accordance with Helsingør Municipality's own explanation - that the municipality has not made a separate assessment of what risks to students 'rights and freedoms will be in the processing of students' personal information, the use of the purchased Chromebooks, the creation of the students as users thereof and the use of the programs in G-Suite as well as the additional programs, contains,

The Danish Data Protection Agency further assumes that the municipality has not carried out a coverage, testing and / or testing of configurations, and consequent personal data flows that arose from the use of the relevant Chromebooks and G-Suite applications, which were made available to the students.

The Danish Data Protection Agency notes that the lack of documentation of the considerations about risks to the data subject's rights, and the assessments of the processing carried out, means that Helsingør Municipality has not been able to demonstrate compliance with Article 5 (1) of the Data Protection Regulation. 1, letter c, with regard to what personal data was necessary at the time of user creation. In this connection, the Danish Data Protection Agency has placed special emphasis on the municipality itself subsequently finding that it was possible to minimize the information and still meet the purpose of the processing. In addition, Helsingør Municipality has not been able to demonstrate compliance with Article 5 (1) of the Data Protection Regulation. 1, letter f. The Danish Data Protection Agency has hereby placed special emphasis on the fact that the municipality has not been able to demonstrate which configuration took place at commissioning and thus could demonstrate that at this time sufficient security was ensured in the treatments that took place.

On this basis, the Danish Data Protection Agency finds that the Municipality of Elsinore has violated Article 5 (1) of the Data Protection Ordinance. Article 5 (2) 1, letter c and letter f.

4.3 G-Suites Additional Products

It is the Data Inspectorate's opinion that the processing authority in the Folkeskole Act cannot cover situations where personal data is used for other than the necessary realization of the purpose in the Folkeskole Act, nor can it legally be passed on to other data controllers for their purposes. This also includes that the students' use of the equipment and the programs do not

generate personally identifiable information, including metadata information used for marketing and profiling, including in particular that the information will not be used for marketing either directly as targeted to the individual student or indirectly as part of a group (class, grade, school, etc.).

In accordance with the information provided by the Municipality of Helsingør, the Danish Data Protection Agency assumes that personal data has been processed in G-Suites' additional products, with the consequent risk of unintentional disclosure of the student's personal data, as well as the possibility of passing on information to a third party - without that this was intended by the municipality - after specifically permitted by the students' parents.

The Danish Data Protection Agency finds that such a transfer cannot be considered necessary for the municipality's exercise of authority. The processing that has taken place in G-Suites' additional products, and has resulted in the transfer of personal data to Google, has therefore not had the necessary processing authority.

On that basis, the Danish Data Protection Agency finds that Helsingør Municipality has violated Article 5 (1) of the Data Protection Ordinance. Article 6 (1) (a)

4.4 Risks and consequences

The Danish Data Protection Agency assumes that Helsingør Municipality has not carried out an analysis of which ones risks the changes to Google's Terms of Use could have for school students if they used the G-suite and its add-on products, including Youtube.

The Danish Data Protection Agency is of the opinion that the use of new complex technology, including software, especially in the field of education where the registered are children and young people, is generally in the area where the Authority considers that it usually involves a high risk for these students' rights and freedoms. In the specific case where in choosing Chromebooks and the technologies used to deliver the system support, it is common knowledge that part of the business model for other parts of Google's products is information gathering, targeted marketing and sales of this information, these conditions will have to be included in the assessment of the risks in question.

In view of this, the Danish Data Protection Agency is of the opinion that there has been a high risk of the data subjects' rights and freedoms. The conditions for carrying out an impact assessment in accordance with Article 35 of the Data Protection Regulation are therefore met.

By not doing so, Helsingør Municipality has violated Article 35 (1) of the Data Protection Act. 1.

The Danish Data Protection Agency is of the opinion that concrete risk assessment and impact assessment - before handing out IT equipment to students and processing students' information - is essential in order to determine which security measures are necessary to implement a security level that suits these risks and which consequences the processing of students' personal data may have for those concerned. The Danish Data Protection Agency must state that several of the above-mentioned violations could have been avoided by making an assessment of the risk of the processing, and a subsequent action on these findings.

4.5 Violation of personal data security and processing security

Based on Helsingør Municipality's own explanation, the Danish Data Protection Agency assumes that there have been several cases where Helsingør Municipality has used students' protected full names instead of an alias, which is otherwise the municipality's procedure. There has been a risk that the students' full names - if the students in question had used the social media that they accessed via their school account - would be published on these media, which is why the Authority finds that there has been a breach of personal data security, see Article 4 (12) of the Data Protection Regulation.

4.6 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.

The Danish Data Protection Agency assumes that Helsingør Municipality - in some cases - has provided the students' computers with an indication of the student's login information, whereby anyone who gained access to the computer could log in to it and gain access to the student's other data and personal information. , just as it would be possible i.a. to post or tag on Youtube or other media in the student's name. Such a procedure typically means that the note is not removed and login information is thus not kept confidential.

It further follows from Article 32 that the data controller shall implement appropriate technical and organizational measures to ensure, inter alia: sustained confidentiality and integrity of processing systems and services, which in the opinion of the Danish Data Protection Agency has not been fulfilled, as the data controller has provided computers handed out to school students with visible login information.

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.

The Danish Data Protection Agency is of the opinion that the requirement pursuant to Article 32 for appropriate security will normally mean that in systems with a large number of confidential information about a large number of users, higher demands must be placed on the data controller's care in cases where personal data is published. including ensuring that there is no unauthorized disclosure of particularly personal or sensitive personal data.

Furthermore, the Danish Data Protection Agency is of the opinion that all probable error scenarios should be tested in connection with the commissioning of new programs where personal data is processed.

Based on the above background, the Data Inspectorate finds that Helsingør Municipality - by not conducting a risk analysis to identify the risks access to G-suite's additional products would entail for the students, Not having performed an analysis of what consequences it could have that school students had access to G-suite add-ons, including Youtube, not having adequately tested the scope and operation of G-suite add-ons prior to their commissioning, not ensuring that names of students with name and address protection were anonymized and not providing adequate safeguards against unauthorized use use of the computers provided to the school pupils - has not taken appropriate organizational and technical measures to ensure a level of security appropriate to the risks involved in the processing of personal data by the Municipality of Helsingør, cf. Article 32 (1) of the Data Protection Regulation. 1.

notification of the breach.

The Danish Data Protection Agency further finds that Helsingør Municipality's assessment that no notification should be made, cf. Article 33 of the Data Protection Act, as it was unlikely that the breach of personal data security could involve a risk to natural persons' rights or freedoms, is clearly unfounded in the facts. The Danish Data Protection Agency has emphasized here that there are several breaches, several of which have manifested a realized risk. The Municipality of Elsinore should therefore, within 72 hours after the municipality had become aware of the breach of personal data security, have reported this to the Danish Data Protection Agency.

As a result, Helsingør Municipality has not complied with the requirements of Article 33 (1) of the Data Protection Regulation. 1.

4.8 Summary

When choosing a response, the Danish Data Protection Agency has emphasized, immediately, ensuring that Helsingør

Municipality's processing is brought in accordance with the Data Protection Ordinance.

The Danish Data Protection Agency therefore issues an order to Helsingør Municipality to bring the processing using Chromebooks in accordance with the regulation, cf. Article 58 (1) of the Data Protection Regulation. 2, letter d. This must be done by Helsingør municipality before 1 November 2021, make the following: Risk assessment of the treatments in Chromebooks and G-Suite, which reflects the flows of personal data the treatments entail, The risk assessment must partly treat the necessary options for to configure the product and address the questions about the scope of the legal basis in the Primary and Lower Secondary School Act in relation to the use required of the pupils. If the risk to the data subjects and their liberties is assessed as being high, the order also includes the preparation of an impact assessment.

The Danish Data Protection Agency issues a warning to the municipality of Helsingør that the use of G-Suites 'supplementary programs without carrying out data protection law impact assessment will be contrary to the Data Protection Ordinance, unless it is proven by the now mandated assessment that the risk to data subjects' rights and freedoms is not high. . The warning is issued in accordance with Article 58 (2) of the Data Protection Regulation. 2, letter a.

The Danish Data Protection Agency has noted that Helsingør Municipality has closed students 'access via school accounts to G-Suites' supplementary programs, including Youtube.

If the assessments of the risk made by Helsingør Municipality show a high risk to the data subjects' rights and freedoms, and these risks have not been reduced to a level less than high before the order deadline expires on 1 November 2021, the Danish Data Protection Agency hereby announces a temporary limitation of the treatments, such that treatments involving a high risk, after this date, must not take place as long as the risk has not been reduced to a level lower than high. The processing restriction is notified in accordance with Article 58 (2) of the Data Protection Regulation. 2, letter f.

Failure to comply with an order or a temporary restriction may, unless a higher penalty is due, be punished by a fine or imprisonment for up to 6 months, cf. section 41 (1) of the Data Protection Act. 2, No. 4.

For the violations found, the Danish Data Protection Agency, in addition to the already chosen corrective measures, expresses serious criticism that the Municipality of Helsingør's processing of personal data has not been in accordance with the Data Protection Ordinance

Article 5, paragraph Article 5 (2) 1, letter c and letter f.,

Article 5, paragraph Article 6 (1) (a)

Article 32 (1), (1), (33) 1 and 35, para. 1.

5. Concluding remarks

The Danish Data Protection Agency notes that it is the responsibility of Helsingør Municipality to correct and delete information in accordance with the decision. The municipality must therefore contact the parents of the registered children in order to carry out the corrections, anonymisations or deletions of the registered personal data that the parents cannot make themselves in the systems where the students' personal data has been inadvertently published or passed on.

The Danish Data Protection Agency notes that the Danish Data Protection Agency's decision cannot be appealed to another administrative authority, cf. section 30 of the Data Protection Act.

The Danish Data Protection Agency's decision may, however, be brought before the courts, cf. section 63 of the Constitution.

The Danish Data Protection Agency hereby considers the case closed and does not take any further action in the case.

Appendix: Legal basis

Excerpt from Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC (General Regulation on data protection).

Article 2, para. This Regulation shall apply to the processing of personal data carried out in whole or in part by means of automatic data processing and to other non-automatic processing of personal data which are or will be contained in a register.

Article 4. For the purposes of this Regulation:

'Personal data' means any information relating to an identified or identifiable natural person ('the data subject'); identifiable natural person means a natural person who can be directly or indirectly identified, in particular by an identifier such as a name, identification number, location data, an online identifier or one or more elements specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

'Processing' means any activity or series of activities - with or without the use of automatic processing - to which personal data or a collection of personal data are made, e.g. collection, registration, organization, systematization, storage, adaptation or modification, retrieval, search, use, disclosure by transmission, dissemination or any other form of transfer, assembly or interconnection, restriction, deletion or destruction;

[…]

'Data controller' means a natural or legal person, a public authority, an institution or any other body which, alone or in conjunction with others, decides on the purposes and means by which personal data may be processed; if the purposes and means of such processing are laid down in Union or national law of the Member States, the controller or the specific criteria for its designation may be laid down in Union or national law of the Member States;

[…]

'Breach of personal data security' means a breach of security which results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data transmitted, stored or otherwise processed;

Article 30. Each data controller and, where applicable, the data controller's representative shall keep records of processing activities under their responsibility. These lists must include all of the following information:

name and contact details of the data controller and, if applicable, the joint data controller, the data controller's representative and the data protection adviser;

the purposes of the treatment

a description of the categories of data subjects and the categories of personal data

the categories of recipients to whom the personal data are or will be disclosed, including recipients in third countries or international organizations;

where applicable, transfers of personal data to a third country or an international organization, including the declaration of that third country or this international organization and, in the case of transfers pursuant to Article 49 (2), 1, second paragraph, documentation of appropriate guarantees

if possible, the expected deadlines for deleting the different categories of information

where possible, a general description of the technical and organizational security measures referred to in Article 32 (2). 1.

Article 32. Taking into account the current state of the art, the cost of implementation and the nature, scope, coherence and purpose of the processing concerned, as well as the risks of varying probability and seriousness of natural persons' rights and freedoms, the controller and processor shall take appropriate technical and organizational measures to ensure level of security appropriate to these risks, including as appropriate:

pseudonymization and encryption of personal data

ability to ensure lasting confidentiality, integrity, availability and robustness of treatment systems and services;

ability to timely restore the availability of and access to personal data in the event of a physical or technical incident;

a procedure for regular testing, assessment and evaluation of the effectiveness of technical and organizational measures to ensure treatment safety.

PCS. 2. In assessing the appropriate level of security, particular consideration shall be given to the risks posed by processing, in particular in the event of accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data transmitted, stored or on otherwise treated.

PCS. Compliance with an approved code of conduct referred to in Article 40 or an approved certification mechanism referred to in Article 42 may be used as an element to demonstrate compliance with the requirements of paragraph 1 of this Article. 1.

PCS. The Data Controller and the Processor shall take steps to ensure that any natural person performing the work of the Data Controller or Processor and who has access to personal data only processes it on the instructions of the Data Controller, unless processing is required under EU the law or the national law of the Member States.

Article 33. In the event of a breach of personal data security, the controller shall, without undue delay and if possible within 72 hours after becoming aware of it, report the breach of personal data security to the supervisory authority competent in accordance with Article 55, unless this is unlikely; , that the breach of personal data security involves a risk to the rights or freedoms of natural persons. If the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by a reason for the delay.

PCS. 2. The data processor shall notify the data controller without undue delay after becoming aware of a breach of personal data security.

PCS. 3. The one in para. The notification referred to in paragraph 1 must at least:

describe the nature of the breach of personal data security, including, if possible, the categories and approximate number of data subjects concerned, as well as the categories and approximate number of personal data records concerned;

provide the name and contact details of the data protection adviser or another contact point where further information can be obtained

describe the likely consequences of the breach of personal data security

describe the measures taken or proposed by the data controller to deal with the breach of personal data security, including, where appropriate, measures to limit its potential harmful effects.

PCS. 4. When and to the extent that it is not possible to provide the information in aggregate, the information may be communicated step by step without undue further delay.

PCS. 5. The data controller shall document all breaches of personal data security, including the facts of the breach of personal data security, its effects and the remedial measures taken. This documentation must enable the supervisory authority to verify compliance with this article.

Article 34. Where a breach of personal data security is likely to involve a high risk to the rights and freedoms of natural persons, the controller shall without undue delay notify the data subject of the breach of personal data security.

PCS. The notification of the data subject in accordance with paragraph 2 of this Article. Paragraph 1 must describe in clear and comprehensible language the nature of the breach of personal data security and contain at least the information and measures referred to in Article 33 (1). 3 (b), (c) and (d).

PCS. It is not necessary to notify the data subject as referred to in paragraph 1. 1, if one of the following conditions is met:

the data controller has implemented appropriate technical and organizational protection measures, and these measures have been applied to the personal data affected by the breach of personal data security, in particular measures that make the personal data incomprehensible to anyone who has not authorized access to it, such as encryption

the data controller has taken subsequent measures to ensure that the high risk to data subjects' rights and freedoms referred to in paragraph 1 1 is probably no longer real

it will require a disproportionate effort. In such a case, a public announcement or similar measure must be taken instead, informing the data subjects in a similarly effective manner.

PCS. 4. If the data controller has not already notified the data subject of the breach of personal data security, the supervisory authority may, after considering the likelihood that the breach of personal data security involves a high risk, require the data controller to do so or decide that one of the conditions in PCS. 3 are met.