The Danish Data Protection Authority maintains the ban in the Chromebook case

Date: 18-08-2022

Decision

Public authorities

Prohibition

Reported breach of personal data security

Treatment safety

Children

Basic principles

Risk assessment and impact analysis

In a much publicized case about the use of Google Workspace in Helsingør Municipality, the Data Protection Authority has now dealt with the material that the municipality has recently supplied. Against this background, the Danish Data Protection Authority maintains the ban that was lifted in July.

Journal number: 2020-431-0061

Summary

In a new decision, the Danish Data Protection Authority maintains the processing ban against Helsingør Municipality's use of Google Workspace, which the Danish Data Protection Authority lifted in mid-July.

This is done on the basis of a careful review of the extensive material that Helsingør Municipality has sent to the inspectorate on 1 August. According to the Danish Data Protection Authority's assessment, the municipality has still not documented that it has reduced the high risks for the children in the municipality's schools.

"Teachers and students are currently in a difficult situation where they cannot use the tools they usually use. Our decision in no way prohibits the use of IT in schools - but the specific use of certain tools in the municipality is not justifiable the children's information. And to put it somewhat squarely, it is a consequence of the municipality's selection and non-selection over several years," says Allan Frank, who is an IT security specialist and lawyer at the Norwegian Data Protection Authority, and continues:

"The goal here is not to live up to some opaque bureaucracy, but to take care of the students' information. According to the

GDPR, children are entitled to special protection. As adults, we can each freely choose which digital services we want to use, but children must now once again use the tools that the public schools make available to them. And therefore it is important that the municipalities ensure that the children's information is not used for purposes other than those permitted by the Public Schools Act - for example marketing, profiling or product development."

The ban concerns - as in the previous decision - only Helsingør Municipality.

Main points in the Data Protection Authority's new decision

The Danish Data Protection Authority - like Helsingør Municipality - assumes that several of the processes involve a high risk for the people who use Google Workspace.

Helsingør Municipality is of the opinion that all the relevant risks have been identified and handled, but the Data Protection Authority assesses that this is not the case. In the eyes of the Danish Data Protection Authority, the municipality has not assessed the relevant risks that appear in the contract with the supplier itself, and other publicly known risk issues in the technology they have chosen. In addition, the risks that the municipality has identified have not been sufficiently reduced.

Helsingør Municipality has assessed that Google only acts as a data processor, but in the opinion of the Danish Data Protection Authority, Google acts in several areas as an independent data controller that processes personal data for its own purposes. This is based, among other things, on the fact that, according to the municipality's material, Google perceives itself as the data controller in a number of areas.

The Danish Data Protection Authority finds that the material from Helsingør Municipality does not meet the content requirements for an impact analysis. For example, the municipality has not assessed the relevant risks - not even for the treatments described - and has only partially described the necessary safety measures.

The Norwegian Data Protection Authority has not been able to establish that Helsingør Municipality's data protection advisor has indicated that he has comments on the impact assessment.

In summary, the Danish Data Protection Authority's assessment is that Helsingør Municipality cannot reduce the risk to an acceptable level without changes to the contract basis and the technology the municipality has chosen to use.

What can Helsingør Municipality do now?

If Helsingør Municipality wishes to use Google Workspace in the schools in the future, the municipality should, in cooperation with its suppliers, manage the relevant risks for the children's personal data - including those that the Danish Data Protection

Authority has pointed out in the three decisions - and prepare a consequence analysis.

If the municipality here recognizes that it is not fully possible to reduce every high risk, there is an option in the GDPR to draw up a plan for legalization together with the Data Protection Authority.

The Norwegian Data Protection Authority is already proposing that the municipality and the supervisory authority meet as soon as possible to discuss the next steps in more detail, so that students and teachers can return to normal everyday life as soon as possible in a responsible manner.

What about the other municipalities?

Although the decision specifically relates to the processing of personal data in Helsingør Municipality, the Data Protection Authority encourages other municipalities with similar circumstances to look at the same areas as in this case - especially in relation to unauthorized disclosure and transfer to unsafe third countries. Here, the task is to assess whether there are similar problems in the individual municipalities, and if so, in cooperation with the suppliers, to get control of the treatments so that the equipment can be used in accordance with the rules.

According to the GDPR, it is the individual municipality that is responsible for the data. But the Danish Data Protection Authority encourages people to raise in groups, so that the municipalities join together - possibly. under the auspices of KL or relevant line ministries - to solve the problems. Many of the conditions will be comparable or similar.

Although the municipalities are responsible for the data, there is also an important task for the suppliers chosen by the municipalities. They must help to document the use and change the terms and technology where necessary. This applies to suppliers in general - but in this specific case the Danish Data Protection Authority has also been in dialogue with Google and directly encouraged the company to play an active role in finding solutions that can reduce the risk to the children.

Decision

The Danish Data Protection Authority hereby returns to the matter, where Helsingør Municipality reported a breach of personal data security to the Danish Data Protection Authority on 29 January 2020. The report has the following reference number: ce0e5422ddfb3fefaa9f621cfa0f129127058500.

1.1. The decision of 10 September 2021

On 10 September 2021, the Danish Data Protection Authority made a decision regarding Helsingør Municipality's breach of personal data security. The Data Protection Authority found, among other things, that there was a basis for expressing serious

criticism that Helsingør Municipality's processing of personal data using Google Chromebooks had not been done in accordance with the data protection regulation[1] article 5, subsection 2, cf. Article 5, subsection 1, letters c and f, and Article 5, subsection 1, letter a, cf. Article 6, subsection 1, and Article 32, subsection 1, Article 33, subsection 1, and Article 35, subsection 1.

Furthermore, the Danish Data Protection Authority found grounds to notify the Municipality of Helsingør of an order to bring its processing of personal data using Google Chromebooks in line with the data protection regulation. This should be done by Helsingør Municipality carrying out a risk assessment of the processing activity before 1 November 2021, which reflects the flows of personal data that the processing entails. The risk assessment was partly to deal with the necessary options for configuring the product and partly to investigate the authority in the Folkeskole Act for the municipality's requirement for students to use Google Chromebooks in schools. If the risk to the rights and freedoms of the registered persons was assessed as being high, the municipality had to carry out a consequence analysis as part of the order. The order was announced in accordance with the data protection regulation's article 58, subsection 2, letter d.

The Danish Data Protection Authority also found that there was a basis for issuing a warning to Helsingør Municipality that use of Google G-Suite's add-on programs without carrying out an impact analysis regarding data protection, cf. the regulation's article 35, subsection 1, would probably be in violation of the data protection regulation.

Finally, the Data Protection Authority found grounds to notify the Municipality of Helsingør of a temporary restriction on the processing activity, if the assessments of the risks that the municipality had been ordered to carry out showed a high risk to the rights and freedoms of the data subjects, and the municipality had not reduced these risks before the expiry of the injunction period to a level less than high. The limitation meant that processing of personal data that entailed a high risk for the rights and freedoms of the data subjects must not take place as long as the risks had not been reduced to a level lower than high.

As a follow-up to the Danish Data Protection Authority's decision of 10 September 2021, by letter of 10 November 2021, Helsingør Municipality sent the municipality's risk assessment regarding the use of Google Chromebooks and G-Suite for Education to the Danish Data Protection Authority, just as the municipality sent additional documentation to prove the legality of the processing activity. In response to a request of 2 December 2021 from the Data Protection Authority, Helsingør Municipality also sent a number of additional information in the case on 9 December 2021.

1.2. The decision of 14 July 2022

On 14 July 2022, the Danish Data Protection Authority made a new decision regarding Helsingør Municipality's processing activities using Google Chromebooks and Workspace for Education. In this decision, the Danish Data Protection Authority found grounds to notify Helsingør Municipality of a ban on processing personal data using Google Chromebooks and Workspace for Education. The ban applied until Helsingør Municipality had brought the processing activity in line with the data protection regulation - as stated in the decision - and prepared adequate documentation for this.

In addition, in the decision, the supervisory authority suspended any transfer of personal data to the USA that Helsingør Municipality has instructed Google Cloud EMEA Limited to carry out as a data processor for the municipality, until Helsingør Municipality could demonstrate that the rules in Chapter V of the Data Protection Regulation had been observed.

The ban and suspension came into effect immediately, but Helsingør Municipality was granted a deadline of 3 August 2022 to include and terminate users and rights as well as delete already transferred information.

The ban and suspension were announced in accordance with the data protection regulation's article 58, subsection 2, letters f and j.

The Danish Data Protection Authority also found grounds for expressing serious criticism that Helsingør Municipality's processing of personal data had not taken place in accordance with the data protection regulation's article 5, subsection 2, cf. Article 5, subsection 1, letter a, Article 24, cf. Article 28, subsection 1, Article 35, subsection 1, as well as article 44, cf. article 46, subsection 1.

2. Decision

As a follow-up to the Danish Data Protection Authority's decision of 14 July 2022, Helsingør Municipality has on 1 August 2022 sent a document entitled "Impact analysis for Google Chromebooks and G-Suite for Education" with annexes to the Danish Data Protection Authority, including a revised risk assessment.

After a review and assessment of the material that Helsingør Municipality sent to the Data Protection Authority on 1 August 2022, the Authority finds that Helsingør Municipality's processing of personal data using Google Chromebooks and Workspace for Education is still not in accordance with the data protection regulation, including that the documentation of 1 August 2022, which Helsingør Municipality has prepared, is not in accordance with the data protection regulation, article 35, subsection 1, and subsection 7, and Article 36, subsection 1.

Against this background, the Danish Data Protection Authority's ban of 14 July 2022 is upheld.

However, the ban is changed so that the Danish Data Protection Authority notifies Helsingør Municipality of a ban on processing personal data using Google Chromebooks and Workspace for Education. The ban applies until Helsingør Municipality has brought the processing activity in line with the data protection regulation, as stated in the Danish Data Protection Authority's decision of 14 July 2022, and has carried out an impact analysis regarding data protection that meets the requirements for content and process for its implementation, which are found in the regulation's article 35 and 36. For treatments where prior consultation with the Data Protection Authority is required pursuant to Article 36 of the Data Protection Regulation, the prohibition applies until the Authority has issued an opinion pursuant to Article 36, subsection 2, and Helsingør Municipality has taken the necessary measures on the basis of the Danish Data Protection Authority's opinion, or until the Danish Data Protection Authority permits the processing at a time before the opinion is available.

The ban, which is announced pursuant to the data protection regulation, article 58, subsection 2, letter f, enters into force immediately.

According to the Data Protection Act[2] § 41, subsection 2, no. 4, whoever fails to comply with a temporary or definitive restriction of processing notified by the Danish Data Protection Authority pursuant to Article 58, subsection of the Data Protection Regulation shall be punished with a fine or imprisonment for up to 6 months. 2, letter f.

The Norwegian Data Protection Authority also reserves the right to use additional powers pursuant to Article 58, subsection of the Data Protection Regulation. 2, for conditions described in this decision, when Helsingør Municipality has presented final documentation which fully explains the legality of the processing and the risks for the rights and freedoms of the data subjects. In addition, the above-mentioned conditions may also be subject to sanctions under Section 41 of the Data Protection Act.

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

3. Case presentation

In continuation of the Data Protection Authority's decision on 14 July 2022, Helsingør Municipality has on 1 August 2022 forwarded new material in the case in the form of the document "Impact analysis for Google Chromebooks and G-Suite for Education" with four appendices:

Revised risk assessment

Settings of Google Chromebooks and G Suite for Education v. 1.0 dated 29 July 2022 applicable to one school in the municipality and copy of that identical settings were set for all schools in the municipality

Document package consisting of audit reports, contract terms, Google Whitepapers and Google User Data Requests

Schematic review of issues and implemented mitigating measures

3.1. Helsingør Municipality's comments

In its forwarding email of 1 August 2022, Helsingør Municipality has, among other things, stated the following:

"Enclosed is the municipality's impact analysis, which takes a position on the questions raised. As an appendix to the impact analysis, there is, among other things, a large number of screenshots in Appendix 2 documenting the municipality's settings. The total documentation consists of several hundred screenshots. However, due to the number here, the municipality has only attached screenshots for one school to illustrate these settings, but if the Norwegian Data Protection Authority wishes to receive all these screenshots, the municipality will be happy to send them. […]

Since the school year for the municipality's school-seeking children begins on 8 August 2022, and since the use of the Services is a crucial prerequisite for being able to deliver the planned education in the 2022/2023 school year, it is of course of great importance for the municipality to have the ban withdrawn. […]

For the sake of clarity, it should be noted that even if the municipality's students attend the new school year on 8 August 2022, the municipality will not hand over computers and provide access to the Services for the new students in the 0th grade. […]"

From the Helsingør Municipality's document "Impact analysis regarding Google Chromebooks and G-Suite for Education" from August 2022, it appears, among other things, following:

"Description of the treatment activities

1. The nature, scope, context and purpose of the treatments

A digital learning platform based on Google Chromebooks with Workspace for Education Standard is used for teaching. The platform enables the sharing of documents between students and teachers and generally enables collaboration within the class and across classes.

Information contained in the Services relates to students and teachers.

As a starting point, neither sensitive information, CPR numbers nor information about criminal offenses related to the students or teachers are processed via the systems. However, it cannot be ruled out that this information may be included in e-mails from the teachers or via other material, and instructions have also been given to the teachers to prevent this. This must therefore be considered highly unusual and unintentional.

This is personal data related to students, who generally enjoy special protection according to the data protection rules, as students of compulsory school age are considered a vulnerable group of people given the students' age.

Helsingør Municipality works purposefully to prepare children and young people for the society and labor market of the future as part of the municipality's solution to the tasks of offering education. All grade levels work daily with IT as an integral part of teaching in all subjects to support professional learning in the subjects and the students' digital skills, which underlines the necessity of the treatment.

In order to ensure the schools and students a future sustainable model for IT-supported teaching, the municipality has chosen the Services as the municipality's teaching platform.

Personal data, recipients and the period of time in which the personal data is stored

The following types of personal data are processed in the following way in order to solve the teaching task.

Personal information Name, Unilogin, class, email address (username, unilogin + domain), school, material produced, emails sent and pictures (profile pictures or in material).

Recipients Internal: Teachers, administrators, students. External: Wizkids and Google as data processor

Time period for storage Data is stored until a student either changes municipality - or three months after the student leaves after finishing school (cell J9 in the risk analysis).

Systematic description of the treatment activity

KL describes the general treatment activity for the school area as follows:

"The processing of personal data takes place for the purpose of organizing the school year, including student assessments, well-being measurements, compensation claims from students and student declarations.

Personal data is also processed in connection with school boards, including members and remuneration for members and advisory bodies, including student councils, parents' councils and pedagogical councils.

More:

A digital learning platform based on Google Chromebooks with the Workspace for Education Standard - Services is used for teaching. The platform enables the sharing of documents between students and teachers and generally enables collaboration within the class and across classes.

From "cradle to grave" this can be systematically produced as follows:

Treatment of physical machine

Purchase of physical machine/Chromebook

Delivery to student/parents

Return from student/parents

Redistribution (after power wash)/destruction

Account creation and administration of the municipality's overall Google account

Creation and configuration of account (e.g. where data is stored)

Selection of facilities (core only)

Backup

Logging of activities (students, teachers and admins)

User administration and system monitoring

Creation of classes (automatically via TEA)

Creation of students (automatically via TEA)

Creating aliases for name-protected students (manually. Until then they are on hold).

Reporting of students' and teachers' use of GWfES

When a student leaves Helsingør Kommune folkeskole, it is registered in TEA and the student's data is deleted after 3 months

(automatically)

Teacher activities

Creation and storage of lesson plans, assignments, questionnaires (Classroom, Drev)

Evaluation of assignments (Classroom, Drive)

Chat (Hangouts, Meet)

Student activities

Creation and storage of tasks (Drev), reading lesson plans

Write and hand in the assignment and read the evaluation

Chat (Hangouts, Meet)

The assets on which the personal data depends (hardware, software, networks, people, paper, paper shipping channels) are

identified.

Chromebook (browser is "client" for cloud solution)

Workspace for Education Standard (set up as data center Europe) (part of cloud solution)

Google's data center (part of cloud solution)

School network

Admins (the municipality's IT school supporters)

Wizkids

School secretaries (TEA student administration platform, aliases)

Teachers

Pupils

Assessment of risks and description of measures to counter them

The prepared risk assessment is attached as appendix 1 to this impact assessment under the lines "privacy by design" and "use of data for unintended purposes". The documentation for the implemented mitigation measures is attached as appendices 2 and 3.

Legality and the rights of data subjects

The legality of the treatments

[…]

It appears from the Danish Data Protection Authority's decision of 14 July 2022 that the municipality has not sufficiently ensured Google's role as a data processor in relation to Google's access to personal data, including particularly in the case of ordinary use of Google Chromebook's operating system and Google Workspace's interaction with Google's backend, and that the municipality has not provided the necessary guarantees that Google will meet the requirements of the data protection regulation, cf. the regulation's article 24, cf. article 28, paragraph 1.

It is the municipality's assessment that the measures described in the risk assessment prepared in October 2021 will usually be sufficient to document that Google acts solely as a data processor and in accordance with this role.

It should be noted that the municipality is not otherwise familiar with the practice of the Norwegian Data Protection Authority, which in other cases requires corresponding documentation in relation to the use of a data processor who does not have a

"previous history" of acting outside the framework of the data processor role.

In the Danish Data Protection Authority's decision of 14 July 2022, this critical position towards Google as a data processor is, as far as the municipality can assess, not substantiated. However, after the decision, the Danish Data Protection Authority orally referred to the fact that practice from the Netherlands casts doubt on whether Google processes personal data from the Services in the field of education for its own, commercial purposes, which are irrelevant and inappropriate in relation to the use of the Services in this area.

As part of the work with this impact analysis, the municipality has therefore also provided information on which points of criticism have been leveled against Google in the Dutch case[3]. More specifically, it concerns the following general questions per February-March 2021:

Lack of purpose limitation of Customer Data

Lack of purpose limitation of Diagnostic Data

Lack of transparency in relation to Customer Data

Lack of transparency in relation to Diagnostic Data

Lack of authorization for Google to process personal data as data controller

Lack of control over the way Google processes personal data

Lack of control over the processing of personal data by Google's subcontractors

Lack of opportunity for registrants to gain insight

The municipality understands the Dutch DPIA to mean that these questions essentially concern challenges linked to Google being fully or partially the data controller, that Google demanded the right to process personal data as a data processor as part of its services for purposes that were difficult to reconcile with the Services, and that the processing of e.g. cookie and telemetry information involved processing that was non-transparent.

In appendix 4, for the sake of completeness, the municipality has assessed a number of issues that were raised in the Dutch case. This review shows that these issues have very limited relevance in relation to Helsingør Municipality's use of the Services, as the roles and set-up are decisively different. A major reason for this is, among other things, that the municipality only uses the Core Services, and that Google therefore only has a role as a data processor and thus only processes personal data for the municipality's purposes. Google has unequivocally acknowledged this role in this case (among other things in the

data processing agreement and the attached documentation in Annexes 2 and 3) with the limitations that follow from this.

These issues are thus not relevant in this case, because in this case Google only acts as a data processor and does not process personal data for its own purposes or require access to process personal data for more general purposes that are not limited to the municipality's interest in the processing.

The municipality has therefore chosen to focus the mitigating measures on documenting that Google is the only data processor and only processes personal data as a data processor for the purposes that follow from the municipality's instructions when Google processes personal data as a data processor for the municipality.

A more schematic overview of the potential problems indicated in the Dutch decision and the associated DPIA with a corresponding indication of how the Municipality of Helsingør has mitigated these problems is provided as appendix 4 to this impact assessment.

These mitigating measures are the following:

Documentation is attached that the municipality has chosen settings that ensure that the municipality only uses Core services, cf. appendix 2. These settings imply that Google only has a role as a data processor and that Google alone may act within the municipality's instructions and thus cannot legally carry out its own purposes.

Documentation has been obtained in the form of independent third-party declarations that Google as a data processor does not pursue its own purposes, cf. appendix 3. This documentation ensures that an independent third party has audited Google's processing of personal data as a data processor, and thereby that Google as a data processor acts within for the instructions given, and that Google does not carry out its own purposes contrary to the data processing agreement.

This impact analysis provides an overview of the investigations and considerations that the municipality has carried out in connection with the questions raised, and assesses whether the treatment on the basis of the above entails a high risk.

It appears from the risk assessment that the processing in relation to the rights and freedoms of the data subjects with these mitigating measures has a medium risk which the municipality can accept. It is noted in this connection that the risk is scored at 8, which is the lowest score in the medium risk category. It should also be noted that the primary reason why the risk is not lower is that it involves the processing of information about school pupils of compulsory school age, and that children enjoy special protection in the data protection legal regulations. The risk for school pupils is thereby mitigated to an acceptable level.

Overall, it is the municipality's assessment that the two risks identified in the Data Protection Authority's decision have been

mitigated to an appropriate, acceptable level.

Basic conditions and legal processing

In order to be able to process personal data in the Services as part of the solution of the statutory teaching task, the municipality must have a legal basis for processing personal data.

Although it follows from the Primary Schools Act that the municipality must offer education to children of compulsory school age – and the processing of personal data is a prerequisite for this – it is the municipality's assessment that the Primary Schools Act is not the only basis for this processing, rather than the actual legal basis.

As described above, the Services generally only process non-confidential personal data. Confidential or sensitive information is thus expected not to be processed, and if it happens, it is unusual, unsystematic and unintentional. This impact analysis therefore focuses on the intended processing of general personal data.

This intended processing takes place to solve tasks in the interest of society and as part of the exercise of public authority that the municipality is charged with (the teaching obligation). This implies that the data protection regulation's article 6, subsection 1, letter e, constitutes the processing basis for the processing of personal data in the Services.

In relation to the principles for the processing of personal data, the Danish Data Protection Authority has stated that the municipality has not demonstrated that the processing is legal, fair and transparent. According to the decision, this is because the municipality

Has not included the risk scenarios that may arise as a result of the data processor design and the system choices made in its risk assessment

Have not carried out sufficient testing of the scope and operation of the selected hardware and used software

Unable to document how the municipality controls Google's access to the personal data, including particularly during ordinary use of Google Chromebook's operating system and Google Workspace's interaction with Google's backend in relation to the options for separation of personal data that can take place in accordance with the [data processing agreement]

As stated above, it is explained in more detail why these issues have limited relevance in this case. As also stated, the municipality has also attached documentation which describes in more detail why, in the municipality's assessment, Google does not have a realistic opportunity to blur the line between its role as a data processor and Google's own purposes, which differ from providing services to the municipality, cf. annexes 2 and 3.

The municipality understands applicable law to mean that contractual obligations can also constitute mitigating measures. The municipality will therefore, for the sake of order, also refer to the data processing agreement with Google[4], where the following is stated:

"5.2 Scope of Processing.

5.2.1 Customer's Instructions. Customer instructs Google to process Customer Personal Data only in accordance with applicable law: (a) to provide, secure, and monitor the Services and TSS; (b) as further specified via Customer's use of the Services (including the Admin Console and other functionality of the Services) and TSS; (c) as documented in the form of the Agreement (including this Data Processing Amendment); and (d) as further documented in any other written instructions given by Customer and acknowledged by Google as constituting instructions for purposes of this Data Processing Amendment (collectively, the "Instructions").

5.2.2 Google's Compliance with Instructions. Google will comply with the Instructions unless prohibited by European Law.

5.2.3 Instruction Notifications. Google will immediately notify Customer if, in Google's opinion: (a) European Law prohibits Google from complying with an Instruction; (b) an Instruction does not comply with European Data Protection Law; or (c) Google is otherwise unable to comply with an Instruction, in each case unless such notice is prohibited by European Law. This Section does not reduce either party's rights and obligations elsewhere in the Agreement.

5.3. Additional Products. If Google at its option makes any Additional Products available to Customer in accordance with the Additional Product Terms, and if Customer opts to install or use those Additional Products, the Services may allow those Additional Products to access Customer Personal Data as required for the interoperation of the Additional Products with the Services. For clarity, this Data Processing Amendment does not apply to the processing of personal data in connection with the provision of any Additional Products installed or used by Customer, including personal data transmitted to or from such Additional Products. Customer may use the functionality of the Services to enable or disable Additional Products, and is not required to use Additional Products in order to use the Services."

As previously described, the municipality does not use the Additional Services, and the data processor agreement is thus very clear in relation to the fact that Google alone has a role as a data processor and that Google alone can process personal data for the municipality's purposes.

The total amount of mitigating measures in the form of the data processing agreement with Google, the municipality's settings

etc., cf. appendix 2, Google's supplementary documentation, cf. appendix 3, and the assessment of the relevance of the Dutch case, which the Data Protection Authority has referred to, cf. appendix 4, implies that, in the municipality's assessment, there is sufficient documentation for the municipality to have demonstrated that the processing is legal, reasonable and transparent.

In this connection, the municipality also notes that this documentation should not be assessed in a vacuum. The fact that the Services are undoubtedly covered by the scope of the data protection regulation and the competence of the Danish Data Protection Authority, the agreed obligations for Google by virtue of the data processing agreement and the municipality's instructions and Google's documentation that Google lives up to these obligations, combined with a more general contractual obligation for Google over for the municipality, the overall result is that Google, by processing information contrary to this, would expose itself to a very large risk of fines and compensation claims.

In addition to the principle of lawful processing, the municipality will also specifically refer to the principle of data minimization. In the risk assessment, this is treated as a separate question in row 11, and it is the municipality's assessment that this principle is also observed.

The rights of the data subjects

The municipality has drawn up privacy policies and procedures which contribute to securing the rights of data subjects. The municipality thus informs the registered about the processing. The municipality will [in addition to] information in the privacy policy on the website send a renewed information letter to the employees.

The municipality also has procedures for handling access requests as well as requests from the registered for correction and deletion, etc. The procedures ensure that the municipality responds to a request from a registered person without undue delay and at the latest after one month, unless the request is complicated, after which the response deadline can be extended by a further two months.

Particularly in relation to the handling of requests from the registered, the municipality's procedures are supported by the data processing agreement with Google, where the following is stated:

"9.2 Data Subject Requests.

9.2.1 Responsibility for Requests. During the Term, if Google's Cloud Data Protection Team receives a request from a data subject that relates to Customer Personal Data and identifies Customer, Google will: (a) advise the data subject to submit their request to Customer; (b) promptly notify the Customer; and (c) not otherwise respond to that data subject's request without

authorization from Customer. Customer will be responsible for responding to any such request including, where necessary, by using the functionality of the Services.

9.2.2 Google's Data Subject Request Assistance. Google will (taking into account the nature of the processing of Customer Personal Data) assist Customer in fulfilling its (or, where Customer is a processor, the relevant controller's) obligations under Chapter III of the GDPR to respond to requests for exercising the data subject's rights by:

providing Additional Security Controls in accordance with Section 7.1.3 (Additional Security Controls);

complying with Sections 9.1 (Access; Rectification; Restricted Processing; Portability) and 9.2.1 (Responsibility for Requests); spirit

if subsections (a) and (b) above are insufficient for Customer (or the relevant controller) to comply with such obligations, upon Customer's request, providing Customer with additional reasonable cooperation and assistance."

On this basis, it is the municipality's assessment that the use of the Services will be able to secure the rights of those registered. […]

Monitoring and updating

The impact analysis is reviewed at least once a year, and is also reviewed if it is assessed from a risk-based approach that there may be significant changes regarding the covered treatment activities.

The views of the data subjects

As part of the impact analysis, the data controller must, if relevant, obtain the views of the data subjects or their representatives. These views can be obtained using different means depending on the situation. It is up to the data controller to choose how this should take place. For example, focus groups, questionnaires, presentation to the employees' representatives or consultation of a relevant organization can be used. If the data controller's final decision differs from the data subject's views, the authority's or company's justification for proceeding or not must be described.

This impact analysis is precisely based on a complaint from a parent and the Danish Data Protection Authority's decisions. Helsingør Municipality has therefore not, on the basis of a professional assessment, found it relevant to include additional views from the registered or their representatives.

Presentation to DPO

This impact assessment has been submitted to the municipality's DPO, Bech-Bruun, in August 2022.

[…]

Appendix 3 – Documentation that Google, as a data processor, does not fulfill its own purposes

ISO 27001 certification

Google is ISO 27001 certified[5]. This certification by Google as an organization implies a requirement that Google complies with applicable legislation and requirements. This concerns, among other things, about the following

Section 4.2 Understanding stakeholders' needs and expectations, where it appears from point b that the organization must determine stakeholders' requirements that are relevant to information security. The municipality adds that this also deals with requirements in connection with concluded contracts, see further below.

Annex A: A5.1 Guidelines for managing information security, from which it appears that the purpose is "to provide guidelines for and support information security in accordance with business requirements and relevant laws and regulations".

Annex A: A18.1 Compliance with legal and contractual requirements, from which it appears that the purpose is "to prevent [the organisation's] violation of legal, official or contractual requirements in relation to information security and other security requirements".

The mentioned requirements must be complied with in order to fulfill the conditions for obtaining certification.

Google's additional warranties and information, which are inserted below:

Customer Questions

Google Responses

1) Can Google guarantee that Google does not, when it acts as data processor for Helsingør Municipality, process Customer Data or other personal data for which Helsingør Municipality is data controller for marketing purposes?

Our customers' data is theirs, not Google's. Google only processes Customer Data in accordance with the contracts with customers, and specifically commits in the Google Workspace for Education Terms of Service that Google does not process Customer Data for its own purposes, including for advertising purposes.

Google's commitment to process Customer Data only in accordance with customer contracts and for no other purpose is also subject to audit by an independent third party auditor (currently, EY). For example, Google's latest SOC 2 report de-scribes various tests performed by EY regarding the Control 22 description "The organization only processes customer data in accordance with the applicable data processing terms and does not process customer data for any other purpose", with no

deviations being noted.

Please see our response to question 6 for further instructions on how to download our SOC 2 report and other compliance-related resources.

For users in primary and secondary schools, Google does not use any user personal information (or any information associated with a Google Workspace for Education Account) to target advertising, whether in Google Workspace Core Services (such as Gmail or Calendar), Chrome Education Upgrade , or other Google services accessed while using a Google Work-space for Education account.

2) Can Google confirm that when the settings in Google Workspace and Google Chromebooks are set to make sure that only Core Services are used and available and that Additional Service are disabled, then Google will only process personal data as data processor and not for other purposes than the ones instructed by Helsingør Municipality?

When Additional Services are disabled and only Workspace Core Services are used:

Google processes Customer Personal Data as a processor and only under your instructions. As mentioned in our response to question 1, we do not process Customer Data (including Customer Personal Data) for our own purposes (including advertising purposes), and this commitment is subject to audit by our independent third party auditor.

Google processes Service Data as a controller for limited purposes in accordance with our Google Cloud Privacy Notice. As per our Notice, Service Data is the personal information we collect or generate during our provision and administration of the Google Workspace services, excluding Customer Data. We have provided more information about the purposes for which we process Service Data in our response to question 3 below.

3) Does Google as a data processor process Diagnostic Data, including telemetry, cookies, etc. for other purposes than the one instructed by Helsingør Municipality?

If “Diagnostic Data” (as described in your question) contains personal data, then that is classified as “Service Data” when it has been collected or generated through the Workspace Core Services.

Google may process this Service Data as a controller for the limited purposes described in section "Why we process data" of the Google Cloud Privacy Notice.

4) When Google provides online technical support, can such support be initiated by Google on its own initiative, or will it only be initiated on request by Helsingør Municipality?

We understand "online technical support" to refer to our Technical Support Services for Google Workspace.

As explained in our Google Workspace Subprocessors URL, Technical Support Services are "customer-initiated", and would not be initiated by Google since, by their nature, Technical Support Services are dependent on a request from a customer.

This article describes how your administrator can contact Google directly for support.

5) Will it in the near future be possible as a general Google feature to opt out of online technical support from insecure third countries?

First, we would like to clarify that each Subprocessor we engage goes through a rigorous selection process to ensure it has the required technical expertise and can deliver the appropriate level of security and privacy. We provide the same contract commitments for all Subprocessors in Section 11 of our Data Processing Amendment.

As noted in our response to question 4, we understand "online technical support" to refer to our Technical Support Services for Google Workspace.

Google continues to invest heavily on features to offer enhanced geo-location control over data. At the moment, to be able to offer 24/7 Technical Support Services as part of the 'follow the sun' support model, these services may be provided from locations outside the EU/EEA.

However, as stated in our Google Workspace Subprocessors URL:

· each Third Party Subprocessor providing Technical Support Services “only has access to Customer Data if Customer explicitly elects to share Customer Data in the course of a support case (e.g. screen-shots)”.

· Google Group Subprocessors providing Technical Support Services “may require limited, authorized access to Customer Data to respond to Customer-initiated requests”.

Our customers can rely on our Standard Contractual Clauses (as well as our supplementary measures) as a legal mechanism to meet their compliance needs with regards to the transfer of Customer Personal Data (i.e. the personal data comprised in Customer Data) outside the EU.

6) If possible, Helsingør Municipality will appreciate any documentation, including documentation from third parties such as audits, etc., to support the answers provided above.

Compliance Resources

Our Compliance Reports Manager provides you with easy, on-demand access to critical compliance resources. Please go to

https://cloud.google.com/security/compliance/compliance-re-ports-manager/ and sign-in with your Google Workspace account to see all the resources available to you. You may specifically want to review our: • ISO certification (27001, 27017, 27018, 27701) * SOC 1, 2 and 3 audit reports As indicated above, we are also gathering other talking points and resources that may be useful to support your Data Protection Impact Assessment. We will share these with you early next week.

Other Useful Resources Chromebooks

1. ChromeOS 1-Pager

2. ChromeOS (ISO 27001, 27017/18, SOC1)

* Chrome Enterprise Upgrade

* Chrome Education Upgrade

* Chrome Nonprofit Upgrade

* Chromebook Enterprise

Our Guide on how to customize and implement Google Workspace (including Privacy best practices)

1. Google Workspace for EDU data protection implementation guide

Data Processing Terms & Customer Data Processing Commitments

2. Google Workspace Service-Specific Terms

3. Data Processing Amendment to Google Workspace and/or Complementary Product Agreement

4. Google's adherence to the EU GDPR Code of Conduct

Service Data

5. Google Cloud Privacy Notice

6. Google's commitment on processing of Service Data

Data Transfers and Schrems II ruling

7. Transfer Impact Assessment: How to Assess the Risk of Cloud EEA-U.S.Data Transfers Using European Data Protection Board’s Recommendations (the document is omitted, as the document in its entirety is considered confidential by Google)

8. Google Cloud's implementation of the New EU Standard Contractual Clauses

9. Safeguards for international data transfers with Google Cloud

10. Reaffirming Google Cloud's commitments to EU businesses in light of the EDPB's Recommendations

11. Google Cloud welcomes the EU's new Standard Contractual Clauses for cross-border data transfers

Additional Privacy Resources

12. Privacy Resource Center

13. Google Transparency Report

14. Enhancing our privacy commitments to customers (blog post 2020)

Lack of purpose limitation for customer data

Potential issues

How has Helsingør Municipality mitigated the risk?

Google does not expressly wish to exclude the further processing of Helsingør Municipality's personal data in the role of independent data controller with the aim of revealing illegal activity without first obtaining prior written approval from the Customer. Google does not provide controls to override or avoid scanning, filtering or other analysis of spam and malware where commercially, technically and reasonably possible.

Google is the only data processor, as the municipality only uses Core Services, and Google is thus not responsible for the data. This issue is not relevant. (This is confirmed, among other things, by the data processing agreement and by the ISO 27001 certification.)

The students do not have access to the e-mail function. A check on teachers' use of e-mail is turned on, including [that] attachments are not harmful and that incoming e-mails with attachments are opened in a sandbox. This issue is not relevant.

Google processes personal data as an independent data controller for the purposes of marketing, profiling, data analysis and market research.

The risk is mitigated, as Google has contractually committed itself not to process information for these purposes, as the municipality only uses Core Services, cf. the data processing agreement section 5.

There is a risk that machine learning to improve the content of spelling and grammar data is not limited to Helsingør Municipality's own domain

The municipality is the data controller, i.e. processing of texts etc. happens for the purpose of the municipality. In addition, metadata reporting is switched off so that Google has access to identifiable personal data in connection with machine learning.

When Google anonymizes information and subsequently uses it, the anonymization is not sufficient.

Google has stated that the anonymization takes place as prescribed in the WP29 guidelines.

Lack of purpose limitation for diagnostic data

Potential issues

How has Helsingør Municipality mitigated the risk?

Google processes diagnostic data (including telemetry data), support data, feedback data and all settings/configurations selected by Enterprise customers for a wide range of own purposes.

Diagnostic data and feedback are turned off as documented in Appendix 2.

Google does not follow the recommended measures to include Chrome Enterprise in the G Suite Enterprise offering or include separate Chrome browser with "data processor" on Android devices and Chromebooks (where it is not realistic to install another browser).

Google is the only data processor, as the municipality only uses Core Services, and Google is thus not responsible for the data. This issue is not relevant. (This is confirmed, among other things, by data processor agreements and the ISO 27001 certification.)

No legal basis for Google

Potential issues

How has Helsingør Municipality mitigated the risk?

Google does not want to become a data processor for diagnostic data, support data and feedback data.

Google is the data processor and diagnostic data and feedback are turned off as documented in Appendix 2.

Regarding the legal basis for collecting cookie and telemetry data from end-user devices, Google states that Google uses cookies and similar technologies that are necessary for the services to function.

Diagnostic data and feedback are turned off as documented in Appendix 2. In addition, Google is the only data processor, and the legal basis is therefore determined by the municipality.

Default privacy settings that do not promote integrity

Potential issues

How has Helsingør Municipality mitigated the risk?

It is not possible to change Google's default settings, which means that Helsingør Municipality cannot protect personal data via

privacy by default.

The municipality's choice of settings promotes privacy by design as documented in the risk assessment and the attached documentation for settings, and the municipality finds the available options for settings in the Services sufficient, cf. appendices 1 and 2.

Lack of control sub-processors

Potential issues

How has Helsingør Municipality mitigated the risk?

It is not possible to control Google's sub-data processors via audits or similar.

Google is the data processor for Helsingør Municipality in this case, and the municipality supervises Google as data processor and, to the extent necessary, with sub-data processors corresponding to the internal procedures for this. Overall, the municipality considers that the data processing agreement provides sufficient opportunity for this.

Lack of insight into personal data

Potential issues

How has Helsingør Municipality mitigated the risk?

There is a risk that Google does not provide the necessary access to the personal data contained in telemetry and cookie data. Diagnostic data and feedback are turned off as documented in Appendix 2. In addition, Google is the only data processor, and the legal basis is therefore determined by the municipality. It should also be noted that in the data processing agreement Google has undertaken to assist in responding to access requests. "

4. Reason for the Data Protection Authority's decision

The Norwegian Data Protection Authority notes at the outset that, in this decision, the supervisory authority has not taken a position on whether Helsingør Municipality has violated the prohibition that the municipality was notified by the supervisory authority's decision of 14 July 2022.

This decision only considers whether – if applicable, to what extent – Helsingør Municipality has demonstrated through the submitted documentation that the municipality can carry out the processing activity in accordance with the data protection rules.

4.1. Relevant rules

This appears from the data protection regulation's article 35, subsection 1, that the data controller – prior to a processing activity – must carry out an analysis of the consequences of the intended processing activities for the protection of personal data. This applies if the processing, in particular through the use of new technologies and due to its nature, scope, context and purpose, is likely to entail a high risk for the rights and freedoms of natural persons.

Of the regulation's article 35, subsection 2, it also follows that the data controller must consult with the data protection adviser, if one has been appointed, when a data protection impact analysis is carried out. The provision has a natural connection with the regulation's article 39, subsection 1, letter c, from which it appears that the data protection adviser, as a minimum, i.a. tasked with advising on the impact assessment and monitoring its completion when requested under Article 35.

Article 35 of the Data Protection Regulation also contains a number of minimum requirements that an impact analysis must meet as a minimum. These requirements appear from the provision's subsection 7 and includes:

a systematic description of the planned treatment activities and the purposes of the treatment

an assessment of whether the treatment activities are necessary and proportionate to the purposes

an assessment of the risks for the rights and freedoms of the data subjects as referred to in subsection 1, and

the measures envisaged to address these risks, including guarantees, safeguards and mechanisms that can ensure the protection of personal data and demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other affected persons.

In addition, it appears from the data protection regulation's article 35, subsection 11, that the data controller, at least when there is a change in the risk posed by the processing, must assess whether it is necessary to carry out a renewed review to assess whether the new processing is covered by impact analyzes that have already been carried out.

Finally, it appears from the regulation's article 36, subsection 1, that the supervisory authority must be consulted before processing if a consequence analysis shows that the processing will lead to high risk in the absence of measures taken by the data controller to limit the risk.

If, by carrying out the impact analysis - and taking the necessary measures - the data controller has thus not been able to reduce the risk to a level that is less than high, the Data Protection Authority must be consulted before the processing is started. This must be done to ensure that the processing is legal and that the data controller has identified the relevant risks for the data subjects and reduced these risks. In this connection, the Danish Data Protection Authority advises the data controller

on whether all relevant risks have been identified and what measures the data controller can take to mitigate these risks, if necessary. The Danish Data Protection Authority can use all its powers in connection with this.

This is thus a significant guarantee of legal certainty for the rights and freedoms of the data subjects. The disregard of this guarantee undermines the Danish Data Protection Authority's - as the competent supervisory authority - opportunities to learn about and monitor the legality of high-risk processing and thus entails a risk of infringement of the rights and freedoms of the data subjects.

The Data Protection Regulation's rules on impact analysis and possible consultation with the Data Protection Authority must ensure that no processing where there is an inherently high risk for the rights and freedoms of the data subjects is initiated without the data controller having worked with and reduced such risks.

A data protection impact analysis is thus a tool that enables the data controller to work with the risks that a processing activity may entail in a systematic way.

An adequate description of the processing activity, cf. Article 35, subsection 7, letter a, is the prerequisite for the data controller to be able to assess and document the legality of the processing activity, cf. subsection 7, letter b.

Similarly, the factual circumstances regarding the processing activity and its legality are a prerequisite for assessing any risks in the form of deviations from the intended, legal processing activity, cf. subsection 7, letter c.

Finally, this risk assessment, cf. point c, is a prerequisite for identifying and taking the relevant and appropriate measures, cf. point d.

The Norwegian Data Protection Authority can also refer to the Norwegian Data Protection Authority's and the Ministry of Justice's guidance on impact assessments from March 2018, which is available on the Danish Data Protection Authority's website. In addition, in October 2017 the European Data Protection Board adopted its "Guidelines for data protection impact assessment (DPIA) and determination of whether the processing is "likely to involve a high risk" according to Regulation (EU) 2016/679", which is also available on the Data Protection Authority's website website in a Danish version.

4.2. Treatments that have a high inherent risk

On 10 September 2021, the Danish Data Protection Authority notified Helsingør Municipality of an order to bring the municipality's processing of personal data using Google Chromebooks and Workspace in line with the data protection rules. If it turned out below that the risk to the rights and freedoms of the data subjects associated with this was high, the municipality

would also have to carry out a data protection impact analysis.

On 10 November 2021, Helsingør Municipality submitted the municipality's risk assessment to the Danish Data Protection Authority with a view to demonstrating that the municipality had brought its processing activity in line with the data protection rules. Helsingør Municipality stated in this connection that it was the municipality's assessment that the municipality was not obliged to carry out an impact analysis regarding data protection, as the municipality did not use Google Workspace Additional Services.

On 14 July 2022, the Danish Data Protection Authority notified Helsingør Municipality of a ban on processing personal data using Google Chromebooks and Workspace until the municipality had brought the processing activity in line with the data protection regulation as stated in the decision, as well as prepared adequate documentation for this.

The Danish Data Protection Authority emphasized that Helsingør Municipality had not fully assessed and documented the risk scenarios that may arise as a result of the use of Google as a supplier and Google Chromebooks and Workspace as a system.

The Danish Data Protection Authority also emphasized that the risk scenarios that the municipality had, however, assessed and documented indicated that there was probably a high inherent risk with the processing activity in question.

In this connection, the Danish Data Protection Authority based its decision of 14 July 2022 on the basis that Helsingør Municipality did not use Google Workspace Additional Products. The Danish Data Protection Authority continues to base this – in accordance with what Helsingør Municipality stated – on.

Helsingør Municipality has in its description of the processing activity, which is reproduced in section 3.1. above, it is stated that Google Chromebooks and Workspace are used in teaching across all grade levels, and that a number of specified personal data about e.g. the students. In the Danish Data Protection Authority's opinion, this is the same processing activity which is also the subject of the Danish Data Protection Authority's decision of 10 September 2021 and 14 July 2022.

It is therefore – as is also apparent from the Danish Data Protection Authority's decision of 14 July 2022 – that the Danish Data Protection Authority's assessment is that Helsingør Municipality's processing of personal data using Google Chromebooks and Workspace probably entails an inherently high risk for the rights and freedoms of natural persons.

This is because new, complex technology, including software, especially in the field of education, where the registered are children and young people, in the opinion of the Danish Data Protection Authority, usually entails a high risk for the rights and freedoms of these students.

The Danish Data Protection Authority notes below that a processing activity such as this contains two of the nine elements which, according to the guidelines of the European Data Protection Board[6], indicate a high inherent risk. Furthermore, the Danish Data Protection Authority is of the opinion that Helsingør Municipality's specific use of Google Chromebooks and Workspace contains a third element that indicates a high inherent risk, in particular that it involves extensive processing of personal data, as the hardware and software in question are used across the municipality's elementary schools.

It is therefore the Danish Data Protection Authority's assessment that Helsingør Municipality is obliged to carry out a data protection impact analysis in accordance with Article 35 of the Data Protection Regulation.

This is also apparent from the Danish Data Protection Authority's decision of 14 July 2022. In this connection, the Danish Data Protection Authority has – as an indication that the processing activity probably has a high inherent risk – assessed in more detail the extent to which information for which Helsingør Municipality is the data controller is processed to others purposes other than those provided for in the Folkeskole Act.

The Norwegian Data Protection Authority has stated the following below:

"It is the opinion of the Data Protection Authority that Helsingør Municipality's processing of personal data pursuant to the Folkeskole Act, cf. the regulation's article 6, subsection 1, letter e, does not cover situations where personal data is processed for purposes other than those provided for in the Folkeskole Act. The information cannot therefore legally be passed on to other data controllers for use for their purposes, when it is a question of purposes that are not provided for in the Folkeskole Act. This also includes the processing of personal data that may occur when students use the equipment and software, including metadata information that is used for marketing and profiling, regardless of whether the information is used for direct marketing and profiling or indirectly as part of a group (class, year , school, etc.)."

It is thus the Danish Data Protection Authority's assessment that the processing activity in question in general – as a result of the presence of three general elements that indicate that the processing activity probably entails a high inherent risk, and based on the specific risk scenario of processing personal data for other purposes – requires, that Helsingør Municipality conducts an impact analysis regarding data protection, cf. Article 35 of the regulation.

In conclusion, the Data Protection Authority notes that it appears from the Data Protection Authority's and the Ministry of Justice's guidance on impact assessments from March 2018 that it is not necessary to carry out an impact analysis for activities that were ongoing at the time when the data protection regulation applied and which were checked by the Data

Protection Authority pursuant to of the currently applicable Personal Data Act rules on reporting obligations in Chapters 12 and 13.

However, it also appears that the data controller – if there is a change to the processing activity – must decide whether, based on the rules of the data protection regulation, an impact analysis must be carried out. This must be read in conjunction with the data protection regulation's article 35, subsection 11, according to which the data controller is obliged to continuously assess whether changes to the processing activity give rise to revising an existing impact analysis, at least when there is a change in the risk posed by the processing activities.

The Danish Data Protection Authority has noted below that there have been changes to the "Service-specific terms for Google Workspace" eight times since October 2020 and changes to the "Data Processing Amendment to Google Workspace and/or Complementary Product Agreement" five times since May 2018. Furthermore, both Since May 2018, Chrome OS and the Chrome browser have been significantly updated a significant number of times from version 67 to 104.

In general, the Danish Data Protection Authority is of the opinion that significant changes in terms, software and applications generally constitute a significant change in the risk posed by the processing activity.

Even if the processing activity in question began before 25 May 2018, it is therefore the opinion of the Danish Data Protection Authority that the obligation for Helsingør Municipality to carry out an impact analysis according to Article 35 of the Data Protection Regulation has been triggered after the regulation came into force and that Helsingør Municipality has been obliged to continuously update this impact assessment.

4.3. Helsingør Municipality's documentation of 1 August 2022

On 1 August 2022, Helsingør Municipality - as a follow-up to the Data Protection Authority's decision of 14 July 2022 - submitted its documentation regarding the municipality's use of Google Chromebooks and Workspace.

The documentation shows, among other things, that it has only been prepared on the basis of the Danish Data Protection Authority's decision of 14 July 2022, and that the documentation must address the risks that the Danish Data Protection Authority has dealt with in its decision of 14 July 2022.

It appears below that in order to meet the questions raised by the Data Protection Authority, Helsingør Municipality has done the following:

"Documentation is attached that the municipality has chosen settings that ensure that the municipality only uses Core services,

cf. appendix 2. These settings imply that Google only has a role as a data processor and that Google may only act within the municipality's instructions and thus cannot legally carry out its own purposes.

Documentation has been obtained in the form of independent third-party declarations that Google as a data processor does not pursue its own purposes, cf. appendix 3. This documentation ensures that an independent third party has audited Google's processing of personal data as a data processor, and thereby that Google as a data processor acts within for the instructions given, and that Google does not carry out its own purposes contrary to the data processing agreement.

This impact analysis provides an overview of the investigations and considerations that the municipality has carried out in connection with the questions raised, as well as assesses whether the treatment on the basis of the above entails a high risk."

As stated above, however, the Data Protection Authority has – as was also the case in the Data Protection Authority's decision of 14 July 2022 – assumed that Helsingør Municipality does not use Additional Services, but only Core Services.

As documentation for (i) that the municipality has sufficiently ensured that Google only processes personal data as a data processor, and (ii) that Google does not process personal data for its own purposes, it has submitted a description of the contractual measures that the municipality has entered into with Google for this purpose, as well as a description of the technical measures that the municipality has taken for the same purpose.

Contractual measures

The Municipality of Helsingør has generally stated that in its delivery of Google Chromebooks and Workspace, Google only acts as a data processor and does not process personal data for its own purposes or require access to process personal data for more general purposes, which are not limited to the municipality's interest in the processing.

The municipality has below referred to the data processing agreement with Google[7], from which the following appears:

"5.2 Scope of Processing.

5.2.1 Customer's Instructions. Customer instructs Google to process Customer Personal Data only in accordance with applicable law: (a) to provide, secure, and monitor the Services and TSS; (b) as further specified via Customer's use of the Services (including the Admin Console and other functionality of the Services) and TSS; (c) as documented in the form of the Agreement (including this Data Processing Amendment); and (d) as further documented in any other written instructions given by Customer and acknowledged by Google as constituting instructions for purposes of this Data Processing Amendment (collectively, the "Instructions").

5.2.2 Google's Compliance with Instructions. Google will comply with the Instructions unless prohibited by European Law. […]”

(The Norwegian Data Protection Authority's emphasis)

Google's data processing agreement also states the following:

"2. Definitions

2.1 Capitalized terms defined in the Agreement apply to this Data Processing

Amendment. In addition, in this Data Processing Amendment: […]

Customer Data means data submitted, stored, sent or received via the Services by Customer or End Users.

Customer Personal Data means the personal data contained within the Customer Data, including any special categories of personal data defined under the European Data Protection Law.”

In addition, Helsingør Municipality has listed a number of questions which the municipality has received answers from Google. This shows, among other things, that Google confirms that processing of "Customer Personal Data" only takes place in accordance with the customer's instructions, and that Google does not process "Customer Personal Data" for its own purposes.

The definition of "Customer Personal Data" includes - as appears from section 2 of Google's data processing agreement - only information that is entered, stored, sent or received via Google Workspace by the customer or end user.

It is the Danish Data Protection Authority's assessment that this definition does not include all possible personal data that is generated through the use of Google Chromebooks and Workspace.

In this respect, the Danish Data Protection Authority has placed particular emphasis on Google's own answer to the municipality's questions 2 and 3, from which the following appears:

”2) Can Google confirm that when the settings in Google Workspace and Google Chromebooks are set to make sure that only Core Services are used and available and that Additional Service are disabled, then Google will only process personal data as data processor and not for other purposes than the ones instructed by Helsingør Municipality?

When Additional Services are disabled and only Workspace Core Services are used:

Google processes Customer Personal Data as a processor and only under your instructions. As mentioned in our response to question 1, we do not process Customer Data (including Customer Personal Data) for our own purposes (including advertising purposes), and this commitment is subject to audit by our independent third party auditor.

Google processes Service Data as a controller for limited purposes in accordance with our Google Cloud Privacy Notice. As per our Notice, Service Data is the personal information we collect or generate during our provision and administration of the Google Workspace services, excluding Customer Data. We have provided more information about the purposes for which we process Service Data in our response to question 3 below.

3) Does Google as a data processor process Diagnostic Data, including telemetry, cookies, etc. for other purposes than the one instructed by Helsingør Municipality?

If “Diagnostic Data” (as described in your question) contains personal data, then that is classified as “Service Data” when it has been collected or generated through the Workspace Core Services.

Google may process this Service Data as a controller for the limited purposes described in section “Why we process data” of the Google Cloud Privacy Notice.” (The Danish Data Protection Authority's emphasis)

With regard to the delimitation of "Service Data", it appears from Google's privacy policy (Google Cloud Privacy Notice) of 20 April 2022 that, among other things, concerns the following:

"Service Data is the personal information Google collects or generates during the provision and administration of the Cloud Services, excluding any Customer Data and Partner Data. Service Data includes:

Cloud payments and transactions. We keep reasonable business records of charges, payments, and billing details and issues.

Cloud settings and configurations. We record your configuration and settings, including resource identifiers and attributes. This includes service and security settings for data and other resources.

Technical and operational details of your usage of Cloud Services. We collect information about usage, operational status, software errors and crash reports, authentication credentials, quality and performance metrics, and other technical details necessary for us to operate and maintain Cloud Services and related software. This information may include device identifiers, identifiers from cookies or tokens, and IP addresses.”

With regard to the purposes of Google's processing of the personal data in question, the following appears from the privacy policy:

"Google processes Service Data for the following purposes:

Provide Cloud Services you request. Service Data is primarily used to deliver the Cloud Services that you and our customers request. This includes a number of processing activities that are necessary to provide the Cloud Services, including processing

to bill for services usage, to ensure services are working as intended, to detect and avoid outages or other problems you might experience, and to secure your data and the services you use.

Make recommendations to optimize use of Cloud Services. We may process Service Data to provide you and our customers with recommendations and tips. These suggestions may include ways to better secure your account or data, options to reduce service charges or improve performance, and information about new or related products and features. We may also evaluate your response to our recommendations.

Maintain and improve Cloud Services. We evaluate Service Data to help us improve the performance and functionality of Cloud Services. As we optimize Cloud Services for you, this may improve them for our customers and vice versa.

Provide and improve other services you request. We may use Service Data to deliver and improve other services that you and our customers request, including Google or third-party services that are enabled via the Cloud Services, administrative consoles, APIs, or the Google Cloud Platform Marketplace or Google Workspace Marketplace.

Assist you. We use Service Data when needed to provide technical support and professional services as requested by you and our customers, and to assess whether we have met your needs. We also use Service Data to improve our online support, and to communicate with you and our customers. This includes notifications about updates to Cloud Services, and responding to support requests.

Protect you, our users, the public, and Google. We use Service Data to improve the safety and reliability of our services. This includes detecting, preventing, and responding to fraud, abuse, security risks, and technical issues that could harm our users, our customers, the public, or Google. These activities are an important part of our commitment to secure our services.

Comply with legal obligations. We may need to process Service Data to comply with our legal obligations, for example, where we're responding to legal process or an enforceable governmental request, or to meet our financial record-keeping obligations.

Other purposes with your consent. We may ask for your consent to process information for other purposes not covered in this Privacy Notice. You have the right to withdraw your consent at any time.

To achieve these purposes, we may use Service Data together with information we collect from other Google products and services. We may use algorithms to recognize patterns in Service Data. Manual collection and review of Service Data may also occur, such as when you interact directly with our billing or support teams. We may aggregate and anonymize Service Data to eliminate personal details, and we may use Service Data for internal reporting and analysis of applicable product and

business operations."

In other words, a number of additional information is thus generated and collected – in the opinion of the Danish Data Protection Authority – by students' and teachers' use of Google Chromebooks and Workspace, which is passed on to Google in order for Google to process this personal data for its own purposes, cf. above.

When Helsingør Municipality decides which tools are used in the municipality's primary schools, including by the individual student, it is the municipality that determines the purposes and aids for the processing of personal data that takes place when using the tools. Helsingør Municipality is thus the data controller for processing personal data about the pupils and teachers in question, which is also apparent from the Data Protection Authority's decision of 14 July 2022.

It also appears from the decision that Helsingør Municipality – as the data controller – cannot process personal data for purposes other than those stipulated in the Folkeskole Act.

The information can therefore also not legally be passed on to other data controllers for use for their purposes, when it is a question of purposes that are not provided for in the Folkeskole Act. This also includes the processing of personal data that may occur when students use the equipment and software.

It is the opinion of the Danish Data Protection Authority that the processing of personal data, which is provided for in the rules of the Folkeskole Act on compulsory education, and thus can take place in accordance with Article 6, paragraph 1 of the Data Protection Regulation. 1, letter e, does not include that the information may be disclosed to other independent data controllers, including for use for purposes such as further development of technology suppliers' applications, etc. The Danish Data Protection Authority is of the opinion that the disclosure of personal data by public authorities to private data controllers generally requires a separate authorization when it is a question of purposes that lie outside the official tasks that the public authority is required to carry out.

In this case, the municipality of Helsingør – as the data controller as a result of its decision that the municipality's primary school students must use the equipment in question – passes on personal data to Google for use for Google's own purposes, which are detailed in Google's privacy policy.

It is thus the Danish Data Protection Authority's assessment that the contractual measures and statements from Google, which Helsingør Municipality has documented, are irrelevant to the matters described in the Danish Data Protection Authority's decision of 14 July 2022.

The Danish Data Protection Authority has in particular emphasized that the Helsingør Municipality's instructions to Google to only process "Customer Personal Data" for the municipality's purposes do not include all the personal data that is processed when the municipality's students use Google Chromebooks and Workspace, and that there are a number of personal data in the form of "Service Data", which is collected and passed on to Google for use for Google's own purposes.

The Danish Data Protection Authority has noted that it is no longer Helsingør Municipality's assessment that it cannot be ruled out that Google acts in breach of its contractual obligations and processes personal data for purposes other than those instructed by the municipality.

Technical measures

Appendix 2 of the documentation shows the technical measures that Helsingør Municipality has taken to prevent and limit the processing of personal data outside of the municipality's instructions. With regard to these measures, it is - after a review - the Danish Data Protection Authority's opinion that these are mainly application settings which prevent or limit the municipality's students and teachers from sharing information with others.

This concerns, among other things, about (i) sharing of documents via dedicated sharing functionality or via shared drives, (ii) restrictions on teachers' access to email attachments, (iii) restrictions on students' access to email in general, (iv) access restrictions on participation in video conferences, (v) access restrictions for calendar information, (vi) restrictions on access to Workspace from third countries, etc.

With regard to restrictions on Google's use of personal data, there are only a few settings that relate to this.

These are (i) the cut-off of the use of private Google accounts on the Chromebooks in question, (ii) the cut-off of the sharing of diagnostic data to Parallels, (iii) the cut-off of access to give Google user feedback regarding the applications used , (iv) sharing data with Google when cleaning up the Chrome browser, (v) cutting off Google's collection of entered web addresses and metadata for the purpose of improving search and browsing.

It is the Danish Data Protection Authority's assessment that the majority of these settings do not limit or prevent the generation and collection of Service Data when using Google Chromebooks and Workspace and its passing on from Helsingør Municipality to Google.

The Danish Data Protection Authority has emphasized that the majority of the settings relate to restrictions on the sharing of information by the municipality's teachers and students with other outsiders, and that the other individual settings only relate to

selected, special functionalities in Google Workspace, including, for example, the access to give Google direct user feedback or collection of entered web addresses.

The Danish Data Protection Authority has also emphasized that the setting that limits the sharing of diagnostic data to Parallels does not cut off the generation and collection of Service Data and its passing on to Google, as the setting concerns the application Parallels, which the Danish Data Protection Authority is aware of is a virtualization application, and thus not Google Chromebooks or Workspace.

Against this background, it is the Danish Data Protection Authority's assessment that the technical measures cannot ensure that personal data is only processed for Helsingør Municipality's purposes.

Overall, it is therefore the Danish Data Protection Authority's assessment that neither the contractual nor technical measures are suitable to address the risks that are central to the submitted documentation.

In addition, it is the Danish Data Protection Authority's assessment that the identified and described risks in themselves do not sufficiently take into account all parts of the processing activity in question.

The Danish Data Protection Authority has emphasized that the identification and description of the identified risks only starts from the top layer of the technology stack in the form of Google Workspace. By not also examining and describing the other elements of Google Chromebooks - such as The Chrome browser and Google OS - Helsingør Municipality has not identified the full extent of the risks.

Furthermore, the Danish Data Protection Authority is of the opinion that Helsingør Municipality – by only dealing with the above-mentioned risks – has not included all relevant processing activities that may entail a high risk for the rights and freedoms of the data subjects.

As stated above, in its decision of 14 July 2022, the Danish Data Protection Authority - as an indication that the processing activity probably has a high inherent risk - has assessed in more detail the extent to which information for which Helsingør Municipality is the data controller is processed for purposes other than those stipulated in the Folkeskole Act.

When there is an indication – a probability – that a processing activity is likely to have a high inherent risk, a data protection impact analysis must be carried out, cf. the regulation's article 35, subsection 1.

It is not sufficient that such an impact analysis only takes into account the individual sub-elements that are likely to involve a high risk. The purpose of the impact analysis, on the other hand, is to describe and assess these – as well as any additional –

risk scenarios.

It is thus not sufficient that Helsingør Municipality has only dealt with the risks to the rights and freedoms of the data subjects in Google Workspace – and not in the entire technology stack, including e.g. The Chrome browser and Google OS.

4.4. Minimum requirements for data protection impact assessments

The Data Protection Regulation's rules on impact analysis and possible consultation with the Data Protection Authority must ensure that no processing where there is an inherently high risk to the rights and freedoms of the data subjects is initiated without the data controller having worked with and reduced such risks.

A data protection impact analysis is thus a tool that enables the data controller to work with the risks that a processing activity may entail in a systematic way. The minimum requirements for an impact analysis appear from the regulation's article 35, subsection 7 and includes:

a systematic description of the planned treatment activities and the purposes of the treatment

an assessment of whether the treatment activities are necessary and proportionate to the purposes

an assessment of the risks for the rights and freedoms of the data subjects as referred to in subsection 1, and

the measures envisaged to address these risks, including guarantees, safeguards and mechanisms that can ensure the protection of personal data and demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other affected persons.

An adequate description of the processing activity, cf. Article 35, subsection 7, letter a, is the prerequisite for the data controller to be able to assess and document the legality of the processing activity, cf. subsection 7, letter b.

Similarly, the factual circumstances regarding the processing activity and its legality are a prerequisite for assessing any risks in the form of deviations from the intended, legal processing activity, cf. subsection 7, letter c. Finally, this risk assessment, cf. letter c, is a prerequisite for identifying and taking the relevant and appropriate measures, cf. letter d.

It is the opinion of the Danish Data Protection Authority that, as part of an impact analysis, before processing begins, the data controller must assess the legality of the processing activity. This follows from letter b of the provision, and involves an assessment of how all relevant provisions of the data protection regulation, including especially chapters II-V, are complied with when the activity is carried out as the activity was intended and designed.

In addition, the data controller must assess whether there are risk scenarios that could imply illegal processing of personal

data. In such risk scenarios, the Danish Data Protection Authority understands possible situations that may arise unintentionally and which involve a deviation from the intended, legal processing activity.

It may, for example, be unintentional processing of personal data that the data controller is not authorized to process. It can also be an accidental collection of more information than is necessary in light of the purpose or an accidental failure to delete information when the data controller no longer needs the information. Likewise, it may be unintentional transfers to third countries or the use of data processors who cannot provide the necessary guarantees for compliance with the data protection regulation.

It is the Data Protection Authority's experience that carrying out and updating an impact analysis and the method for this is a good tool for identifying any illegal processing situations. If the data controller, in connection with carrying out and updating an impact analysis, identifies that the intended or ongoing processing activity does not comply with the data protection rules in one or more ways, the data controller must remedy these. This can typically be done via a change to the contractual basis underlying the processing activity, if other data controllers or data processors are involved, or through a re-design of the processing activity. In the extreme, this may mean that the intended treatment activity in question cannot be initiated or continued with treatments already in progress.

It is thus a prerequisite for assessing any risks of a processing activity that the activity is legal as it is intended and designed.

4.5. Helsingør Municipality's "consequence analyzes regarding data protection"

After a review of Helsingør Municipality's documentation of 1 August 2022, the Data Protection Authority finds that the documentation does not meet the minimum requirements for an impact analysis, cf. the data protection regulation's article 35, subsection 7, letters a-d.

The Danish Data Protection Authority has emphasized that the documentation does not contain an adequate and systematic description of the processing activity, including a technical description of the equipment and the applications that support the processing, cf. 7, letter a. The documentation, on the other hand, only contains an overall description of types of personal data and categories of data subjects as well as an overall indication of the purpose of the processing activity.

The Danish Data Protection Authority has also emphasized that the documentation only generally contains (i) an assessment of the legality of the processing, cf. the regulation's article 5, subsection 1, letter a, with regard to the possible transfer of personal data to Google, (ii) a description of the processing basis underlying the municipality's processing of personal data, as

well as (iii) an overall reference to the fact that the municipality has drawn up policies and procedures to handle the rights of the data subjects.

The documentation therefore lacks, among other things, an adequate assessment of how the processing activity meets the basic requirements in Article 5 of the regulation, which exception in Article 9 of the data protection regulation forms the basis for the municipality's processing of sensitive personal data[8], and how the data subject's rights under Chapter III are specifically observed when using of Google Chromebooks and Workspace.

In addition, the Data Protection Authority has emphasized that Helsingør Municipality has not identified and assessed all relevant risks of the processing activity, that the risks that the municipality has identified have not been adequately assessed, as the starting point is only the top layer of the technology stack rather than the entire technology stack, cf. Section 4.3. above, and that the municipality has only partially described measures related to processing security, cf. Article 32 of the regulation.

It is therefore the Data Protection Authority's overall assessment that Helsingør Municipality – even for the parts of the processing activity that the municipality has described – has not carried out an impact analysis, cf. the data protection regulation's article 35, subsection 1, as the documentation of 1 August 2022 does not meet the minimum requirements for this in the regulation's article 35, subsection 7.

Finally, the Data Protection Authority has noted that Helsingør Municipality's documentation of 1 August 2022 was submitted to Helsingør Municipality's data protection advisor Bech-Bruun in August 2022. However, it is not clear whether, and if so to what extent, the data protection advisor had any comments on the prepared documentation.

The Danish Data Protection Authority has not been able to establish that the data protection adviser has stated that he has any comments on the prepared documentation.

The Danish Data Protection Authority must recommend that Helsingør Municipality includes any contributions from the municipality's data protection advisor in future impact analyses. The comments from the data protection adviser about the advice that is a duty according to the data protection regulation, article 35, subsection 2, is of significant importance in order to document that the data protection adviser has had the opportunity and room to carry out the tasks incumbent upon him according to Article 39 of the Data Protection Regulation.

Finally, the Danish Data Protection Authority notes that the data controller, cf. the regulation's article 38, subsection 1, must ensure that the data protection adviser is involved sufficiently and in a timely manner, which in the Data Protection Authority's

view implies that the adviser – depending on the specific processing activity – should generally be allocated more than one day to review the relevant material.

4.6. Processing carried out without impact analysis and/or prior consultation with the supervisory authority

The Norwegian Data Protection Authority also finds that Helsingør Municipality, by not consulting the Danish Data Protection Authority in connection with the implementation of - what the municipality itself perceived as - an impact analysis, has acted in violation of Article 36 of the regulation.

As stated in section 4.3. above, it is the Danish Data Protection Authority's assessment that the measures that Helsingør Municipality has taken with regard to the transfer of personal data to Google are not suitable to deal with this situation.

In this connection, the Danish Data Protection Authority is of the opinion that Helsingør Municipality, as a statutory actor in an area – the elementary school area – where the processing of personal data can inherently have serious consequences for the data subjects, especially children and young people as is the case in this case, and which according to the data protection rules enjoys special protection, must be expected to have considerable expertise and experience in handling data protection law issues. This applies not least when the municipality decides to use new, complex technology, where the processing of personal data can lead to a multitude of data protection legal issues and often involve high risks.

In the Data Protection Authority's opinion, Helsingør Municipality should have been aware that the contractual and technical measures taken by the municipality were not suitable to deal with the situation in question, and that any risks were therefore not reduced to a less than high level.

As far as an unacceptable residual risk is concerned, the Danish Data Protection Authority can, among other things, refer to the European Data Protection Board's guidelines for impact assessment, from which the following appears:

"An example of an unacceptably high residual risk includes cases where the data subjects may be exposed to significant or even irreparable consequences that they may not be able to overcome (eg: unlawful access to data that could lead to a threat to the lives of the data subjects , dismissal, financial loss), and/or when it seems obvious that the risk will occur (eg: when it is not possible to limit the number of people who have access to the data due to the methods of exchange used, use or distribution, or when a known vulnerability is not addressed).”[9]

Furthermore, the Danish Data Protection Authority is of the opinion that an unacceptably high residual risk may include cases where (i) unauthorized processing may occur, (ii) processing that goes beyond the legal purposes or (iii) repeated breaches of

personal data security. This applies in particular when such cases will obviously occur - either due to the conditions resulting from a contract which have an impact on the processing activity, or due to known conditions in the technology or service used. Against this background, the Data Protection Authority considers that, in connection with the preparation of its documentation, which in the municipality's view constituted an impact analysis, the Data Protection Authority should have been consulted, cf. the regulation's article 36, subsection 1.

4.7. Relevant topics for impact analysis

For Helsingør Municipality's future work with impact assessments regarding data protection, the Data Protection Authority generally refers to the Data Protection Authority's and the Ministry of Justice's guidance on impact analysis, especially chapter 4 on "special cases", as well as the list prepared by the Data Protection Authority pursuant to Article 35, subsection of the Data Protection Regulation. 4, on treatments that always require the preparation of a consequence analysis.

The Danish Data Protection Authority also refers to the European Data Protection Board's guidelines on impact assessments from October 2017[10], including in particular the following:

"Then it is up to the data controller to assess the risks to the rights and freedoms of the data subjects and to identify the intended measures to limit these risks to an acceptable level and to demonstrate compliance with the General Data Protection Regulation (Article 35, paragraph 7, cf. III.C.c). An example could be the application of appropriate technical and organizational security measures when storing personal data on laptops (effective encryption of the entire hard drive, robust key management, appropriate access controls, secured backups, etc.) in addition to the existing policies (notification, consent, right of access , the right to object, etc.). [...]"

The Danish Data Protection Authority is of the opinion that a data controller - in order to make the correct assessment according to Article 35 of the Data Protection Regulation - is obliged to include the elements and the knowledge that is available, both about the processing itself, but also about conditions surrounding the solution and technology , which are chosen to support processing – in this case Google Chromebooks and Workspace. This includes the entire technology stack used for the treatment.

In addition to the directly relevant factual information about the processing activity, including its purpose and proportionality, it will also be relevant to include information about the used data processors and other types of technology suppliers. It is, among other things, relevant to examine:

in particular, the information that appears in all the terms and conditions that appear in the data processing agreement and/or the contract with the technology supplier, and which indicate the conditions under which the service is delivered,

public knowledge of already known risk issues or security weaknesses in the chosen technology or services, and

matters where one's data processor and supplier have already acknowledged that they are either unresolved or outstanding in relation to compliance with the Data Protection Regulation.

Furthermore, it is more specifically relevant for the data controller to examine, for example, whether there are terms in the data processing agreement and/or contract that make it impossible for the data controller to comply with its duties under the data protection regulation. This may, for example, be the case if a binding instruction to the data processor regarding the processing of personal data cannot be given at all – or only with difficulty – or if there are contractual terms which give the data processor the right – as an independent data controller – to process personal data without the data controllers are authorized to do so.

In addition, it is relevant to investigate whether there have been cases where the technology supplier processes personal data for purposes other than the legal purpose of providing the service (regardless of whether the data controller has instructed the supplier in this regard or not). There may also be cases where the data controller does not have the necessary control over the processing of the information, e.g. because the contract structure and terms are complicated or even incomprehensible, or the data controller cannot obtain the necessary overview of how the data processor actually processes the personal data.

It may also be relevant to investigate the technical aspects of the delivery. There may, for example, be cases where - either via the supplier's own information or via publicly available investigations - it turns out that via the service or application provided, processing of personal data takes place to a greater extent than is otherwise immediately on the basis of the contract, and thus is collected, passed on or otherwise processed unjustifiably.

Finally, it is relevant to carry out self-control and (ongoing) verification, assessment and evaluation of the intended treatment activity. It is a requirement in terms of processing security according to Article 32 of the Data Protection Regulation, but can also more generally be a source of the elements and knowledge that should give the data controller the opportunity to (re)assess whether there are risks with the processing activity in question , and how these can be handled if necessary.

Another obvious place is also the follow-up and evaluation of the breaches of personal data security, cf. the regulation's article 33, which the data controller experiences.

With regard to relevant methods and points to be used for carrying out an impact analysis regarding data protection, especially

when using technology suppliers, the Danish Data Protection Authority can refer to the chapters "Kend your services" and "Kend your supplier" in the Danish Data Protection Authority's guidance on cloud from March 2022, which is available on the authority's website, just as the authority can generally refer to ISO/IEC 29 134, which is an internationally recognized standard for carrying out impact analyses.

In light of this, it is not clear to the Danish Data Protection Authority how Helsingør Municipality has not generally and previously assessed that the processing activity in question was generally likely to have an inherently high risk, including especially as parts of this risk could be mitigated.

In this connection, the Danish Data Protection Authority acknowledges that Helsingør Municipality, as shown in appendix 2 of the documentation, has taken a number of measures which – also in the Danish Data Protection Authority's opinion – limit the risks to the rights and freedoms of data subjects when using Google Chromebooks and Workspaces Core Services.

It is also unclear to the Danish Data Protection Authority how the factual information about Google Chromebooks and Workspace, which is publicly available as a result of similar investigations in the Netherlands[11], has "very limited relevance", when a number of the investigations are also relevant to the use of Core Services and not only Additional services.

The Danish Data Protection Authority refers below, among other things, to to Annex 2 for an update of the data protection impact assessment by the Amsterdam University for Applied Sciences and the University of Groningen.[12] This includes, among other things, more information about the personal data that is collected when using Chrome OS and the Chrome browser, regardless of any settings in Workspace.

Likewise, the Danish Data Protection Authority points out that – according to this updated impact analysis[13] – it does not seem possible to mitigate the relevant risk scenarios without changes to the contractual basis underlying Google's delivery of Chromebooks and Workspace, and the technology used for this.

Finally, the Data Protection Authority refers to Google's press release of 17 June 2022 with the heading "New Commitments on the Processing of Service Data for Our Cloud Customers"[14], from which it appears that Google expects to be able to offer the same terms for "Service Data" as for "Customer Data", starting in 2023 and in successive phases in 2024. It also appears from this that Google will work on a change to Chrome OS, which - for the so-called "managed systems" - will also include the Chrome browser. At that time, these services will also be able to be delivered as a "pure" data processor mode.

5. Summary

After a review and assessment of the material that Helsingør Municipality sent on 1 August 2022, the Data Protection Authority finds that Helsingør Municipality's processing of personal data using Google Chromebooks and Workspace for Education is still not in accordance with the data protection regulation, including that the documentation of 1 August 2022, which Helsingør Municipality has prepared, is not in accordance with the data protection regulation, article 35, subsection 1, and subsection 7 and Article 36, subsection 1.

The previously announced ban of 14 July 2022 is therefore maintained, but amended so that the Data Protection Authority notifies Helsingør Municipality of a ban on processing personal data using Google Chromebooks and Workspace for Education. The ban applies until Helsingør Municipality has brought the processing activity in line with the data protection regulation as stated in the decision of 14 July 2022 and has complied with the regulation's article 35, subsection 1 piece. 7 and Article 36, subsection 1. For treatments where consultation with the Data Protection Authority is required pursuant to Article 36 of the Data Protection Regulation, the ban applies until the Authority has issued an opinion pursuant to Article 36, subsection 2, or the supervisory authority permits the processing at a time before the opinion is available.

The ban, which is announced pursuant to the data protection regulation, article 58, subsection 2, letter f, enters into force immediately.

According to the Data Protection Act § 41, subsection 2, no. 4, whoever fails to comply with a temporary or definitive restriction of processing notified by the Danish Data Protection Authority pursuant to Article 58, subsection of the Data Protection Regulation shall be punished with a fine or imprisonment for up to 6 months. 2, letter f.

The Norwegian Data Protection Authority also reserves the right to use additional powers pursuant to Article 58, subsection of the Data Protection Regulation. 2, and sanctions according to § 41 of the Data Protection Act, for the circumstances pointed out in this decision, when final documentation has been presented which fully explains the risks of the processing for the rights of the data subjects.

6. Concluding remarks

As a follow-up to the above – however, independently of the upheld ban – the Data Protection Authority is happy to engage in dialogue with Helsingør Municipality regarding the handling of the mentioned issue. The Data Protection Authority initially proposes to hold a meeting between the Data Protection Authority, Helsingør Municipality and possibly KL and is happy to receive a number of proposals for possible meeting times.

[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 data protection regulation)

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

[3] See DPIA Google G Suite Enterprise, Data protection impact assessment on the processing of personal data on 3 platforms with the Chrome browser and as installed apps, Version 1 – for consultation with the Dutch DPA, 9 July 2020, with update on 12 February 2021, prepared by the Ministry of Justice and Security Strategic Vendor Management Microsoft (DPIA).

[4] Data Processing Agreement to Google Workspace and/or Complementary Product Agreement, July 7, 2022.

[5] Reference is made to Google Cloud: Data Processing Agreement to G Suite and/or Complementary Product Agreement (Version 2.1) of 19.8.2019, https://workspace.google.com/terms/10293019/dpa_terms.html, Annex A: A18.1.

[6] European Data Protection Board Guidelines for Data Protection Impact Assessment (DPIA) and determination of whether the processing is "likely to involve a high risk" under Regulation (EU) 2016/679, p. 12.

[7] Data Processing Agreement to Google Workspace and/or Complementary Product Agreement, July 7, 2022.

[8] The Data Protection Authority refers below to Helsingør Municipality's own description of the processing activity, from which it appears that, among other things, information on student assessments and well-being measurements is processed. In the opinion of the Danish Data Protection Authority, such information will usually include special categories of personal data according to Article 9 of the regulation.

[9] Article 29 Group Guidelines on Data Protection Impact Assessment (DPIA) and determination of whether the processing is "likely to involve a high risk" under Regulation (EU) 2016/679, WP 248, as endorsed by the European Data Protection Board.

[10] Article 29 Group guidelines on data protection impact assessment (DPIA) and determination of whether the processing is "likely to involve a high risk" under Regulation (EU) 2016/679, WP 248, as endorsed by the European Data Protection Board.

[11] In recent years, a number of authorities in the Netherlands have carried out impact analyzes regarding data protection of both Google G Suite Enterprise and Google Workspace for Education. This concerns the analysis prepared by the Ministry of Justice and Security as well as the analysis prepared for the University of Groningen and the Amsterdam University of Applied Sciences and its update.

[12] Update DPIA report Google Workspace for Education of 2 August 2021.

[13] For the sake of clarity, the Danish Data Protection Authority also refers to the original impact assessment of 15 July 2020, updated 12 March 2021 from Groningen University and Amsterdam University of Applied Sciences.

[14] Introducing new commitments on the processing of service data for our cloud customers | Google Cloud Blog