The Danish Data Protection Authority imposes a processing ban in the Chromebook case

Date: 14-07-2022

Decision

Public authorities

Serious criticism

Prohibition

Suspension

Reported breach of personal data security

Children

Treatment safety

Transfer to third countries

Risk assessment and impact analysis

Basic principles

In a case about the use of Chromebooks in Helsingør Municipality, the Danish Data Protection Authority expresses serious criticism and bans transfers to third countries and the use of Google Workspace.

Journal number: 2020-431-0061

Summary

For a long time, the Danish Data Protection Authority has focused on the use of Chromebooks and Google Workspace (formerly G Suite for Education) in the municipalities. The use is widespread nationwide, but concretely the Data Protection Authority has had a pending case in Helsingør Municipality.

Thus, the Data Protection Authority made a decision in September 2021, where Helsingør Municipality i.a. was ordered to carry out a risk assessment of the municipality's processing of personal data in the primary school using Chromebooks and Workspace. The Danish Data Protection Authority has now established, based on the documentation and assessment of the risk for the data subjects prepared by Helsingør Municipality, that the processing does not meet the requirements of the GDPR on several points.

"Helsingør Municipality has done a great and skilled job to map how personal data is used in the primary school, but it also

highlights the data protection legal problems that can be with the big tech companies' ways of solving the task," says Allan Frank, who is an IT security specialist and lawyer at the Danish Data Protection Authority.

The Norwegian Data Protection Authority finds that the municipality has not assessed any concrete risks in relation to the data processor construction. In addition, the data processing agreement states that information can be transferred to third countries in support situations without the necessary level of security.

Seen in light of the decision from September 2021, the Danish Data Protection Authority has now made a decision. It contains, among other things:

Suspension of Helsingør Municipality carrying out processing where information is transferred to third countries without the necessary level of protection

A general ban on processing with Google Workspace until adequate documentation and impact analysis has been made, and until the processing is brought into compliance with the regulation

Serious criticism of the municipality's processing of personal data

The Danish Data Protection Authority draws attention to the fact that many of the conclusions in this decision will probably apply to other municipalities that use the same processing structure. The Danish Data Protection Authority therefore expects these municipalities to take relevant steps themselves based on the decision - even if the Danish Data Protection Authority is currently finalizing a number of cases concerning other municipalities.

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.

On 10 September 2021, the Danish Data Protection Authority made a decision regarding the breach of personal data security.

The Danish Data Protection Authority found that there were grounds for expressing serious criticism that Helsingør Municipality's processing of personal data through the use of Google Chromebooks had not been done in accordance with the data protection regulation's 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 that there was a basis for notifying 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 was to be done by Helsingør Municipality carrying out a risk assessment of the processing activity, 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 to deal with the questions about the scope authorized in the Primary School Act for the use of Chromebooks that the municipality requires of the students. 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 that there was a basis for notifying the Municipality of Helsingør of a temporary restriction on the processing activity, if the assessments of the risks that the municipality was ordered to carry out showed a high risk to the rights and freedoms of the data subjects, and the municipality had not, before the expiry of the injunction period, reduced these risks to a level less than high. The limitation implies that processing of personal data that entails a high risk for the rights and freedoms of the data subjects may not take place as long as the risks have not been reduced to a level lower than high.

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

1. Decision

After a review of Helsingør Municipality's risk assessment and the municipality's documentation in general, the Data Protection Authority finds that there is a basis for notifying Helsingør Municipality of a ban on processing personal data using Google Chromebooks and Workspace for Education. The ban applies until the Municipality of Helsingør has brought the processing activity in accordance with the data protection regulation as stated in this decision, as well as prepared adequate

documentation for this.

In addition, 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 is suspended until Helsingør Municipality can demonstrate that the rules in Chapter V of the data protection regulation have been observed.

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

The bans are announced in accordance with the data protection regulation, article 58, subsection 2, letters f and j.

Violation of a ban announced by the Danish Data Protection Authority is punishable pursuant to section 41, subsection of the Data Protection Act. 2, no. 4, with a fine or imprisonment of up to 6 months, cf. section 41, subsection 1.

The Danish Data Protection Authority finally finds grounds for expressing serious criticism that Helsingør Municipality's processing of personal data has not taken place in accordance with Article 5, paragraph 1 of the Data Protection Regulation. 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. Case presentation

On 11 December 2019, a citizen complained to the Data Protection Authority about Helsingør Municipality's processing of personal data.

Helsingør Municipality confirmed by letter of 6 January 2020 that a parent had complained to the municipality in 2019 that his child had – without his knowledge – created an account for YouTube, whereby the child's name could be published on YouTube.

Helsingør Municipality further stated that the municipality assessed that it was unlikely that the incident had entailed a risk to the rights and freedoms of the data subjects and therefore had not given rise to reporting a breach of personal data security to the Data Protection Authority, cf. the data protection regulation, article 33, subsection 1.

On 29 January 2020, Helsingør Municipality reported the incident to the Danish Data Protection Authority as a breach of personal data security. At the same time, a number of other municipalities made similar reports, which is why the Danish Data Protection Authority treated the cases together, and the Danish Data Protection Authority requested an opinion from the relevant municipalities by letter of 11 March 2020.

The Danish Data Protection Authority made a decision on 10 September 2021 regarding the relevant breach of personal data security, which Helsingør Municipality had reported to the Danish Data Protection Authority. The Danish Data Protection Authority's decision of 10 September 2021 is reproduced above in section 1, just as the decision in its entirety is attached as an appendix.

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

3. Helsingør Municipality's opinion

3.1. Carrying out a risk assessment, including possibly an impact analysis regarding data protection

On 10 November 2021, Helsingør Municipality sent the municipality's risk assessment for the use of Google Chromebooks and G-Suite for Education (Google Workspace for Education).

At the same time, Helsingør Municipality has informed the Danish Data Protection Authority that the municipality does not use Google Workspace's additional services and has, on that basis, assessed that the municipality is not obliged to prepare a data protection impact analysis.

3.2. Processing of personal data for other purposes

The risk assessment shows that, among the risks that Helsingør Municipality has identified when using Google Chromebooks, the risk of "use of data for unintended purposes". The risk is described as follows:

"There is a risk that Google or other third parties use personal data about teachers and students for marketing or other purposes for which Helsingør Municipality, as data controller, does not want personal data to be processed. In particular, contact information, IP address and digital traces (general information) are relevant in this context. It is noted that this is personal data related to students who enjoy special protection according to the data protection rules, which is why the access to and processing of personal data about the students constitutes an additional element in relation to the risk assessment."

Regarding the probability of this risk materializing, the following appears:

"The municipality uses the product Google Workspace for Education Standard, where the municipality is ensured by virtue of

the data processing agreement that data is not used for other purposes, including marketing, provided that the municipality only uses Core Services.

Reference is made to the data processing agreement and Helsingør Municipality's correspondence with Google, where Google has stated the following: "Information as part of the use of Chromebooks and Google Workspace for Education Standard cannot be used by Google for marketing purposes towards a student or students in a class". "There are no ads shown in Google Workspace for Education core services. Also, none of the personal information collected in the core services is used for advertising purposes (ii) Students' username, also in connection with the created Google Workspace for Education account, is only accessible to Google as a data processor, and usage of Chromebooks and Google Workspace for Education – for example viewing YouTube videos – does not lead to the publication of the username". "The school's admin may allow students to access Google services, such as YouTube, that have features that allow users to share information with others or publicly. For example, if you leave a review in Google Play, your name and photo appear next to your activity. And if you share a photo with a friend who then makes a copy of it, or shares it again, then that photo may continue to appear in your friend's Google Account even after you remove it from your Google Account. Remember, when you share information publicly, your content may become accessible through search engines, including Google Search. For additional information on how Workspace for Education data is shared, please see the Workspace for Education Privacy Notice."

Core services (14 services: Classroom, Drive/Docs, G-mail, Chat, Chrome synchronization, Groups, Meet, Vault, To-do list, Jamboard, Calendar, Keep (stickynotes), Tasks, Sites)

Additional services from Google are covered by other terms in the data processing agreement, which means that the municipality cannot give Google instructions on how personal data may be used. Therefore, the municipality has turned off the use of Additional Services.

Conclusion

Based on the measures implemented above, it is Elsinore municipality's assessment that the probability of the risk becoming a reality is low. However, it cannot be completely ruled out that Google breaks the contractual obligations and nevertheless uses personal data for marketing or other unintended purposes for which Helsingør Municipality has not given instructions, cf. the data processing agreement."

3.3. Transfer of personal data to third countries

From the risk assessment, it appears as an additional risk that Helsingør Municipality has identified when using Google Chromebooks and Workspace for Education, the risk of third-country transfers.

The risk is described as follows:

"There is a risk that personal data about students and teachers (basically ordinary personal data, but it cannot be ruled out that sensitive personal data will also be included) will be transferred to unsafe third countries without a necessary transfer basis and without assurance that the third country in question ensures similar data protection rights as in other EU countries."

Regarding the probability of this risk materializing, the following appears:

"Helsingør Municipality, as the data controller for the processing of personal data about students, has implemented the following relevant mitigating measures in order to reduce the likelihood that the described risk will become a reality:

The EU Commission's standard terms have been entered into (transfer basis), as there is a risk of access from the US via support. As an additional basis for this (supplementary measures), a separate Transfer Impact Assessment (TIA) has been prepared in accordance with the requirements of the Danish Data Protection Authority and the EDPB. Reference is made to the relevant prepared TIA.

It should also be noted that Helsingør Municipality has chosen a solution according to which, as a clear starting point, data is only located within the EU in the data centers in question. It is thus only the risk of support access from an unsafe third country that can lead to access from an unsafe third country:

"Settings in Data Regions in Google Workspace for Education Standard ensures that the data center is located within the EU – and additionally: Will there be online access from countries outside of the EU, for example in connection with support."

Conclusion

Based on the measures implemented above, it is Elsinore municipality's assessment that the probability of the risk becoming a reality is low."

Furthermore, Helsingør Municipality has submitted its documentation for compliance with Chapter V of the Data Protection Regulation when using Google Workspace for Education in the form of the municipality's "Transfer Impact Assessment" (hereafter "TIA").

It appears from this that Helsingør Municipality uses Google Cloud EMEA Limited as a data processor with regard to its use of Google Chromebooks and Workspace for Education. The municipality has, via settings in Google Workspace for Education,

ensured that personal data is only stored in data centers located within the EU/EEA.

However, it appears that personal data – notwithstanding the above setting – may be transferred to Google LLC in the USA as part of remote access in connection with support. The transfer takes place on the basis of the EU Commission's standard contract.

Finally, the following appears from section 1.8 regarding the context and purpose of the transfer of personal data:

"As part of Google's cloud solution, Helsingør Municipality is using:

Google Chromebooks and G Suite for Education (now named Workspace), which is used by Helsingør Kommune for the purpose of educating students as part of Helsingør Kommune's public law obligation as a local, public authority to provide education. It is Helsingør Municipality's assessment that this obligation is best managed with Google as supplier of the above services and the Data Protection Authority has accepted this premise pursuant to the governing law in the Folkeskoleloven.

In order for Helsingør Municipality to use the mentioned services and products offered by Google, it is a requirement that Helsingør Municipality transfers the personal data related to the data subjects stated in sections 1.9-1.10 below to Google's cloud. The purpose of the transfer is thus to store the personal in the data centers (cloud), ensure a high security of the personal data as well as management/support from Google."

In the TIA, Helsingør Municipality has – as far as the Danish Data Protection Authority understands – assessed whether the basis for the transfer to the USA in the form of the standard contract is effective in light of the circumstances of the transfer, including an assessment of whether there is legislation and/or practice in the USA that affects the effectiveness of the concluded standard contract.

Of the TIA's section 2.4 thus states the following:

"Based on statistics and other arguments from the data importer/data recipient, how many years in addition to the assessment period will it take before the probability of access by a public authority (that is lawful in the third country) is still only 50: 50?

Based on the following statistics and arguments, it is Helsingør Municipality's assessment that even if additional 50 years were added to the assessment period of 5 years, the probability of an access by a US public authority (that is lawful in the US) that violates the EU law as stated in the Schrems II judgment is still only 50% chance of occurring within this period of 55 years and thus the risk of a lawful access occurring in the assessment period of 5 years is of a more theoretical than practical nature:

A) Google will carefully review each request to make sure it satisfies applicable laws. If a request asks for too much

information, Google will try to narrow it down, and in some cases Google objects to producing any information at all. Google will share the number and types of requests received in the Transparency Report.

B) When Google receives a request from a government agency, Google will send an email to the user account before disclosing information. If the account is managed by an organization, Google will give notice to the account administrator. If Google is legally prohibited from giving notice, it will not do so. If this is the case, Google will provide notice after the legal prohibition is lifted, such as when a statutory or court-ordered gag period has expired.

C) When a Google entity within the EU, as it is the case in this matter, receives data disclosure requests from US government authorities, Google will only provide personal data if doing so is consistent with all of the following: (i) National law in the Member State of establishment, including any applicable EU laws such as the GDPR. Google will therefore require the US authority to follow the same due process and legal requirements that would apply if the request were made to a local provider of a similar service. (ii) International norms, which means that Google will only provide personal data in response to requests that satisfy the Global Network Initiative's Principles on Freedom of Expression and Privacy and its associated implementation guidelines in Google's policies. This includes any applicable terms of service and privacy policies, as well as policies related to the protection of freedom of expression.

D) With regard to requests for information in emergencies, such as if Google reasonably believes that disclosure can prevent someone from dying or from suffering serious physical harm, Google may provide information to a government agency. This includes bomb threats, school shootings, kidnappings, suicide prevention, and missing persons cases. Google will still consider such requests in light of applicable laws and our policies.

F) Statistics

Google GCP/G-Suite Access requests / disclosed Denmark 2019-2020: 0 / 0

Google Workspace Access requests / disclosed Denmark 2019-2020: 1 / 0

Google Global Diplomatic Legal requests: 1

Google Global User data requests / percentage disclosed Denmark 2019-2020:

30 June 2019 Emergency 2 / 50%. Other legal 29 / 52%. Preservation 8 / 45%. 31 December 2019 Emergency 3 / 0%. Other legal 48 / 38%. Preservation 12 / 41%.

30 June 2020 Emergency 5 / 100%

Other legal 80 / 58%. Preservation 34 / 63%. 31 December 2020 Emergency 1 / 100%. Other legal 87 / 75%. Preservation 32 / 41%

Google National Security Letter requests (NSL) and released 2019/2020 total number all countries: 21

Conclusion

Based on this legal approach and these statistics, it is clear that:

It is statistically improbable that Helsingør Municipality will be the target of a request regarding the use of GCP and G-Suite (now named Workspace).

For other services the risk is minimal given the number of requests / disclosures and the total number of users of using services provided by Google in Denmark.

The number of NSL requests is so low that it is statistically without importance.

If personal data are targeted for a request, Google will carry out an honest assessment of the legality based on EU law. This is supported by the statistics of actual disclosures."

It also appears from the TIA's section 3.4 that the personal data transferred to Google LLC in the United States will be available to Google LLC in plain text:

"Is the personal data at issue accessible in the target jurisdiction in clear text by the data importer/recipient or a third party (i.e. the data is either not appropriately encrypted or access to the keys to decrypt is possible)?

Helsingør Municipality's personal data is always encrypted when at rest as Google uses several layers of encryption to protect customer data at rest in Google Cloud products, using one or more encryption mechanisms. Data for storage is split into chunks, and each chunk is encrypted with a unique data encryption key. These data encryption keys are stored with the data, encrypted with ("wrapped" by) key encryption keys that are exclusively stored and used inside Google's central Key Management Service. Google's Key Management Service is redundant and globally distributed.

All data stored in Google Cloud is encrypted at the storage level using AES256. In this connection, Google uses a common cryptographic library, Tink, which incorporates the FIPS 140-2 validated module, BoringCrypto, to implement encryption consistently across almost all Google Cloud products. Consistent use of a common library means that only a small team of cryptographers needs to implement and maintain this tightly controlled and reviewed code.

However, this encryption does not prevent Google personnel from accessing Helsingør Municipality's personal data because

Google has the key to decrypt data. Google LLC in the U.S. is on the contrary not in possession of the decryption key. This implies that Google in the US or other Google entities outside the EU/EEA or third parties cannot access Helsingør Municipality's personal data without approval by the applicable Google entity established in the EU (Google Ireland). Although encryption - and pseudonymisation, which is also used by Google - does not ensure that Helsingør Municipality has complete control of access to personal data in the EU data centre, it serves as a mitigating factor to meet regulatory or compliance obligations, i.e. in accordance with the guidelines from the EDPB."

In addition, it appears from the TIA's section 3.5 regarding the established transfer basis:

"As stated above in section 1.7 above, it follows from Google's Data Processing Amendment to Google Workspace and/or Complementary Product Agreement modified on 24 September 2021 that the 2021 SCC will be the legal basis for transfers (including online access as part of online support) to countries outside the EU/EEA without an adequacy decision. In this connection Google is contractually obliged as processor to comply with comply with the obligations applicable to it under the European Data Protection Law with respect to the processing of Helsingør Kommune's personal data.

Helsingør Municipality has no reason to believe that any Google entity will not comply with the SCC.

furthermore, Helsingør Municipality will evaluate, and continuously monitor, that Google complies with the 2021 SCC by reviewing, for example, audit reports and standard certifications made available. Helsingør Municipality also has the right to carry out a special 3rd party audit if assessed necessary, cf. the DPA."

Finally, it appears from the TIA's section 4.1.1 as regards legislation and/or practice in the United States affecting the effectiveness of the standard contract entered into:

"The data importer/recipient is not subject to a higher interest from a public foreign authority in requesting access to the personal data (i.e., the data importer or potential recipient is not subject to national law facilitating mass surveillance)

Section 702 FISA

The US entity Google LLC may in practice be seen as the parent company for the EU entities providing the services to Helsingør Municipality. Google LLC. may qualify as an Electronic Commutations Service Provider pursuant to Section 702 FISA for its US customers as the term is broadly understood: "any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored ."

However, there is a high likelihood that the data accessible to the Google LLC, is per se excluded from access under Section

702 FISA because it is data that are not transmitted by it but to it for the purpose of providing a support service. Thus, it is a communication targeted to a "U.S. person" for which the intelligence searches are prohibited (see Alan Charles Raul, "Why Schrems II Might Not Be a Problem for EU-U.S. Data Transfers", December 21, 2020, available at https://bit.ly/3qHNMy7 and a full paper from the same author at https://bit.ly/2V9veez with the follow-up post "Transferring EU Data To US After New Contractual Safeguards" of May 17, 2021, available at https://bit.ly/3l12oHZ). In addition, Helsingør Municipality's personal data does not comprise personal data about "U.S. Persons" and US authorities are thus barred from accessing data under Section 702 FISA for this reason as well.

Hence, it likely that Helsingør Municipality's personal data in EU data centers will not be subject to Section 702 FISA.

We understand that this argument may not be shared by everyone and that requests nevertheless may take place in relation to Google, which is why we rate the probability of this argument to be valid very conservatively to be on the safe side.

EO 12.333

Executive Order 12.333 (EO 12.333) authorizes US intelligence agencies to collect foreign “signals intelligence” information, which is information collected from communications and other data passed or accessible by radio, wire and other electromagnetic means (i.e. all data from telecom and IT infrastructure) . EO 12.333 thus permits "surveillance in transit", such as the accessing of data that are not properly encrypted while it is passing over transatlantic cables. As described under section 3.3. above, all personal data will be transmitted with required and strong encryption in transit. It is thus our assessment that the required technical measurement

through encryption means that EO 12.333 will not entail a higher risk for mass surveillance US authorities.”

It appears below that Helsingør Municipality has assessed the probability that the above assessment is correct at 40%.

Based on Helsingør Municipality's letter of 10 November 2021 with annex, the Danish Data Protection Authority requested additional information from the municipality on 2 December 2021. The Danish Data Protection Authority stated below that any transfers of personal data to the USA as part of support - in the Danish Data Protection Authority's view - were intended, notwithstanding that the municipality has assessed this as a risk for support access from the USA.

The Norwegian Data Protection Authority requested, among other things, Helsingør Municipality about a copy of the municipality's transfer basis, any changes to the instructions and data processing agreement with Google, as well as a review of any supplementary measures that the municipality may have deemed necessary.

By letter of 9 December 2021, Helsingør Municipality has - as a clarification of the above-mentioned risk - stated the following:

"The possible transfer to Google - and the associated risk - is connected to Google's setup. That is that even though the municipality has chosen an EU cloud, Google has secured the right to potentially receive support from third countries in the data processing agreement. This is also the reason why Google has established a transfer basis according to the new SCC (from June 2021), which the municipality uses as a basis for its assessment of the risk.

In general, regarding the risk of support in particular, the following factors can generally be taken as a basis: In very special support situations from an uncertain third country, there will be a very limited window in which the supporter can potentially gain access to personal data in clear text. It is very unlikely that in the limited window the supporter will be required by the government [of the unsafe third country] to provide the personal data.

The municipality further notes that it appears from the prepared TIA that the municipality has assessed that the use of Google Workspace for Education is necessary to solve the municipality's tasks according to the Primary Schools Act, that the possibility of support from third countries cannot be opted out when Google is a data processor, and that the municipality has therefore assessed the risk of using Google.

The transfer basis is, as stated, the new SCC (from June 2021)."

With regard to the data sources used, Helsingør Municipality has stated the following:

"We are talking about different "data sources" in relation to the risk assessment and the TIA. The risk assessment is partly based on the fact that the data processing agreement describes the relationship between the parties in more detail, i.e. that Google is a data processor for the municipality, and that Google reserves the right to provide support from third countries, and that the municipality has ensured that the service is delivered from an EU cloud.

The TIA is based on the documents and links listed in the sub-tab in the TIA."

In addition, Helsingør Municipality has stated the following regarding its assessments, which appear from the TIA:

"The assessments in the TIA of the probability that the individual legal arguments hold are an estimate. In this connection, it is the municipality's assessment that the inserted probabilities are conservative, i.e. that the municipality has allowed doubt to benefit the rights and freedoms of the registered persons. If the Data Protection Authority has a different, reasoned assessment of the likelihood that the individual arguments hold, the municipality will be happy to hear about this. It is also noted for the record that the calculated total risk – i.a. based on these arguments, the circumstances surrounding the possible

transfer, published statistics from Google, the practice and the mitigating measures – is quite low. The municipality also undertakes to continuously monitor and evaluate the likelihood that these arguments hold up.

The legality of using Google Workspace for Education under these circumstances is thus not dependent on whether the estimate of the probability of the durability of a single argument cannot be moved with reasoned arguments."

Finally, Helsingør Municipality has sent a large number of documentation regarding the data processing construction with Google Cloud EMEA Limited, including the data processing agreement "Data Processing Amendment to Google Workspace and/or Complementary Product Agreement" dated 24 September 2021.

4. Reason for the Data Protection Authority's decision

In general, the Danish Data Protection Authority is of the opinion that a data controller who uses a data processor – for all processing – must comply with and be able to demonstrate compliance with the Data Protection Regulation and the Data Protection Act, regardless of where in the data processor chain processing takes place.

It follows from the data protection regulation's article 5, subsection 2, from which it appears that the data controller is responsible for and must be able to demonstrate that subsection 1 is observed. This means, among other things, that the data controller is responsible for and must be able to demonstrate that the personal data is processed legally, fairly and in a transparent manner, cf. Article 5, subsection 1, letter a.

Furthermore, it appears from the regulation's article 24, subsection 1, that the data controller must implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is in accordance with this regulation. This must be done taking into account the nature, scope, context and purpose of the processing in question as well as the risks of varying probability and seriousness to the rights and freedoms of natural persons, and the measures must be revised and updated if necessary.

With this decision, the Danish Data Protection Authority has only decided whether - and to what extent - Helsingør Municipality, as the data controller, processes personal data in accordance with the data protection rules. The Danish Data Protection Authority's competence follows from Section 27 of the Data Protection Act and Chapters VI and VII of the Data Protection Regulation, including the Regulation's Article 55, subsection 2.

4.1. Using Google Chromebooks and Google Workspace for Education

This follows from Section 2, subsection of the Folkeskole Act. 1, that the municipal board is responsible for the primary school.

For the primary school, this follows section 18, subsection of the Act. 1, and § 19, that the organization of teaching, including the choice of teaching and working methods, methods, teaching materials and material selection, as well as the payment for this, in all subjects meet the primary school's purpose, goals for subjects and subjects and are varied so that it corresponds to the individual student's needs and prerequisites.

The Danish Data Protection Authority is of the opinion that both the choice about the use of IT in teaching, including which make and software to use, fall within this margin of discretion.

The Danish Data Protection Authority notes below that the data protection rules are technology-neutral, and the Danish Data Protection Authority can only assess the circumstances in which personal data is processed, cf. the data protection regulation, article 2, subsection 1.

While the Primary Schools Act - in the Data Protection Authority's opinion - gives the municipal council the competence to decide on - and if applicable - which IT equipment is to be used in teaching, this use must continue to take place within the framework of the Data Protection Regulation and the Data Protection Act.

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

As also appears from the Data Protection Authority's decision of 10 September 2021, it is the opinion of the Authority that Helsingør Municipality can determine which tools are used in the municipality's primary schools, cf. the Data Protection Regulation, Article 6, subsection 1, letter e. This also applies to the creation of the individual student as a user of such a system.

However, it is still an essential prerequisite that the data protection regulation and the data protection act are otherwise complied with in the processing of personal data that takes place.

4.2. Risk and consequences

The Danish Data Protection Authority generally finds that Helsingør Municipality's risk assessment regarding the use of Google Chromebooks and Workspace for Education addresses the most significant scenarios and threats.

However, the Danish Data Protection Authority is of the opinion that the use of new, complex technology, including software – especially in the field of education, where the data subjects are children and young people – usually entails a high risk for the

rights and freedoms of these students.

In the specific case where it is generally known that the technologies used for the delivery and system support of the selected service – Google Chromebooks and Workspace for Education – are also used to deliver other parts of Google's products, and these are used for information collection, targeted marketing and sale of this information. Such conditions must therefore be included in the assessment of the risks to the rights and freedoms of the data subjects when using Google Workspace for Education.

The Danish Data Protection Authority finds that Helsingør Municipality's risk assessment does not fully document the risk scenarios that may arise as a result of the data processor design and the system choices made. This applies in particular to (i) how the devices and programs used actually handle the collected personal data, as well as (ii) how the Municipality of Helsingør controls Google's access to the personal data, including in particular during ordinary use of Google Chromebook's operating system and Google Workspace's interaction with Google's backend in relation to to the options for separation of personal data, which must take place in accordance with the data processing agreement.

The Danish Data Protection Authority is of the opinion that carrying out a concrete risk assessment and impact analysis - before handing over IT equipment to students and processing the students' information - is a prerequisite for being able to establish and maintain an appropriate level of security. This is because an appropriate level of security must be seen in the light of the risks, including consequences, that the processing of the students' personal data may have for those concerned.

The Norwegian Data Protection Authority notes that several of the above-mentioned non-observances of the data protection rules could have been avoided if Helsingør Municipality had assessed the risks of the processing and taken appropriate measures in light of these risks.

Based on the above background, the Danish Data Protection Authority finds that Helsingør Municipality - (i) by not including the risk scenarios that may arise as a result of the data processing design and the system choices made in its risk assessment, (ii) by not having carried out sufficient testing of the scope and operation of the selected hardware and used software, as well as (iii) by not being able to document how the municipality controls Google's access to the personal data, including in particular in the ordinary use of Google Chromebook's operating system and Google Workspace's interaction with Google's backend in relation to the options for separating personal data, which can take place in accordance with the Data Processing Act – has not demonstrated that personal data is processed legally, fairly and in a transparent manner in relation to

the data subject, cf. the Data Protection Act, Article 5, subsection 2, cf. Article 5, subsection 1, letter a.

4.3. Use of information for other purposes

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 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, including metadata information that is used for marketing and profiling, regardless of whether the information is used for direct marketing against the individual student or indirectly as part of a group (class , year, school, etc.).

The Danish Data Protection Authority assumes that Helsingør Municipality does not use Google Workspace for Education's additional products.

It appears from Helsingør Municipality's risk assessment that personal data collected in core services – according to the data processing agreement – is not used for marketing purposes.

The Danish Data Protection Authority assumes that Helsingør Municipality, as data controller, has assessed that "it cannot be completely ruled out that Google breaks the contractual obligations and nevertheless uses personal data for marketing or other unintended purposes for which Helsingør Municipality has not given instructions cf. the data processing agreement. "

The Danish Data Protection Authority also assumes that Helsingør Municipality also processes personal data of special categories, cf. the regulation's article 9, using Google Workspace for Education.

In this connection, the Danish Data Protection Authority must generally enforce that a data controller – in accordance with the data protection regulation, article 28, subsection 1 – may only use data processors who can provide the necessary guarantees that the person concerned will comply with the data protection rules in connection with their processing of the information on behalf of the data controller.

This implies that an expectation on the part of the data controller that the selected data processor will act in violation of the entered data processing agreement – in itself – means that the data controller cannot use the data processor in question, cf. the regulation's article 28, subsection 1.

However, the Danish Data Protection Authority has assumed that, in its assessment of this risk, Helsingør Municipality only

considers the risk of the data processor acting in breach of the data processing agreement as hypothetical rather than definitely foreseeable.

The Danish Data Protection Authority finds that Helsingør Municipality – in its assessment of this risk – has not documented that Helsingør Municipality in this situation uses a data processor that can provide the necessary guarantees that the person concerned will meet the requirements of the data protection regulation, cf. the regulation's article 24, cf. article 28, subsection 1.

The Danish Data Protection Authority has placed particular emphasis on the fact that there would be a significant loss of rights for the data subjects if the risk in question materialized, and that the municipality has not listed real remedial technical or organizational measures in its risk assessment with a view to mitigating this risk. It is the Datatilsynet's opinion that Helsingør Municipality's reference to the fact that the municipality has confidence that the supplier will generally comply with the agreement does not constitute a necessary reduction of this risk.

The Danish Data Protection Authority also notes that any risk that entails a high consequence for the rights and freedoms of the data subjects – even with relatively low probabilities of the risk materializing – is likely to entail a high risk for the rights of the data subjects, which triggers the obligation to carry out a impact analysis regarding data protection, cf. the regulation's article 35, subsection 1.

In view of this - and Helsingør Municipality's own assessment that it cannot be ruled out that the data processor will act in violation of the data processing agreement - the Danish Data Protection Authority is of the opinion that the situation triggers the duty to carry out a data protection impact analysis, the regulation's article 35, subsection 1.

Against this background - and as Helsingør Municipality has stated that the municipality has not carried out an impact analysis regarding data protection - the Danish Data Protection Authority finds that Helsingør Municipality's processing of personal data has not taken place in accordance with the regulation's article 35, subsection 1.

4.4. Transfers of personal data to third countries

4.5. Transfer of personal data by the cloud infrastructure

The Danish Data Protection Authority has initially noted that it is Helsingør Municipality's view that the municipality has configured its use of Google Workspace for Education in such a way that "data as a clear starting point is only located within the EU in the data centers in question. It is thus only the risk of support access from an unsafe third country that can lead to

access from an unsafe third country."

Elsinore Municipality's basis of agreement with Google, which regulates the processing activity, includes, among other things, "Data Processing Amendment to Google Workspace and/or Complementary Product Agreement" (agreement amendment), dated September 24, 2021.

The addendum to the agreement states, among other things, following:

10.1 Data Storage and Processing Facilities. Subject to Google's data location commitments under the Service Specific Terms and to the remainder of this Section 10 (Data Transfers), Customer Data may be processed in any country in which Google or its Subprocessors maintain facilities. […]

Subprocessors

11.1 Consent to Subprocessor Engagement. Customer specifically authorizes the engagement as Subprocessors of those entities listed as of the Amendment Effective Date at the URL specified in Section 11.2 (Information about Subprocessors). In addition, without prejudice to Section 11.4 (Opportunity to Object to Subprocessor Changes), Customer generally authorizes the engagement as Subprocessors of any other third parties ("New Subprocessors").

11.2 Information about Subprocessors. Information about Subprocessors, including their functions and locations, is available at: https://workspace.google.com/intl/en/terms/subprocessors.html (as may be updated by Google from time to time in accordance with this Data Processing Amendment)."

Clause of the addendum to the agreement 11.2 refers to an overview of sub-processors used for the provision of Google Workspace for Education. The overview shows a large number of sub-processors which are used to provide technical support and which are located in the EU as well as in third countries, including third countries where the EU Commission has not made a decision on the countries' level of protection, cf. Article 45.

The overview also shows a large number of Google's subsidiaries that are used for limited activities in connection with e.g. Google Workspace, and which is also located both inside and outside the EU/EEA.

With this decision, the Danish Data Protection Authority has not decided to what extent the Municipality of Helsingør, by using Google Workspace for Education - in addition to the USA, cf. further below in section 4.6 - transfers personal data to other third countries, notwithstanding that the information is "stored" within EU/EEA.

However, the Data Protection Authority must recommend that Helsingør Municipality - i.a. by reviewing the Google Workspace

"Service Specific Terms", which are referred to in the clause of the agreement addendum. 10.1 - ensures that the information, as part of processing other than "storage", e.g. as part of general service and support of the underlying cloud infrastructure, etc., is not transferred to third countries, unless Helsingør Municipality instructs the data processor in this regard and provides a valid transfer basis.

The Danish Data Protection Authority is of the opinion that the data controller must provide a valid basis for transfer to all third countries to which personal data may be transferred as part of the delivery of a service in accordance with the basis of the agreement, including for service and support.

4.6. Transfer of personal data to the United States

At the outset, the Danish Data Protection Authority notes that - in the opinion of the Danish Data Protection Authority - this is an intentional and directed transfer to the USA for Helsingør Municipality as a result of the agreed possibility to provide support - in or from the USA - with access to personal data.

The rules on transfer to third countries, including the possible grounds for transfer, can be found in Chapter V of the Data Protection Regulation.

The main rule for the transfer of personal data to third countries appears from the general principle in Article 44 of the Data Protection Regulation. It appears from this that:

"Any transfer of personal data which is subject to processing or is planned to be processed after transfer to a third country or an international organization may only take place if the conditions in [chapter V] subject to the other provisions of this regulation are met by the data controller and the data processor, including onward transfer of personal data from the relevant third country or international organization to another third country or another international organisation. All the provisions of this Chapter shall be applied to ensure that the level of protection guaranteed to natural persons under this Regulation is not undermined.'

Any transfer of personal data can thus only take place if the conditions in Chapter V of the regulation are met.

The Danish Data Protection Authority understands the regulation's article 44 as an obligation for both the data controller and the data processor. Both parties are therefore obliged to ensure that a transfer basis is provided that is effective in light of all the circumstances of the transfer. This also applies in cases where, in practice, it is the data processor who has entered into a standard contract in accordance with the regulation's article 46, subsection 2, letter c, with any sub-data processors in third

countries. In that case, the obligation for the data controller in practice consists in ensuring – and being able to demonstrate to the Danish Data Protection Authority – that the data processor has established the necessary transfer basis and that this transfer basis is effective in light of all the circumstances of the transfer, including the implementation of supplementary measures if necessary.

Furthermore, the Danish Data Protection Authority is of the opinion that – subject to the exceptions in Article 49 of the regulation – the wording in Article 44 states that any transfer of personal data may only take place if the conditions in Chapter V are met, combined with the principle that the level of protection , which is ensured by the data protection regulation must not be undermined, must be understood as meaning that any transfer must be covered by necessary guarantees. Thus, it is not sufficient that almost all transfers or a percentage of transfers enjoy the protection provided for in the data protection regulation, unless this is authorized by the regulation.

One of the options for providing a valid transfer basis under Chapter V is by entering into a standard contract adopted by the EU Commission with the organization in the third country to which the information is transferred, cf. the regulation's article 46, paragraph 1, letter c.

It appears below from the case that Helsingør Municipality has instructed its data processor – Google Cloud EMEA Limited in Ireland – to transfer personal data to a sub-data processor – Google LLC – in the USA. The transfer takes place on the basis of an EU Commission standard contract between Google Cloud EMEA Limited and Google LLC in the USA. This standard contract has been used as the basis for transfers to the US since the end of September 2021.

In case C-311/18, Schrems II, the European Court of Justice clarified that the use of the EU Commission's standard contracts presupposes that a level of protection can be ensured for the personal data in the third country in question, which essentially corresponds to the level of protection within the EU/ EEA.[1]

The European Court of Justice further noted that there may be situations where the EU Commission's standard contract does not constitute "a sufficient means to ensure the effective protection of the personal data that has been transferred to the third country in question, in practice. This is particularly the case when the law of that third country allows its public authorities to interfere with data subjects' rights regarding that information."[2]

In such cases where the standard contract, given their nature, cannot provide guarantees that go beyond the contractual obligation to ensure that the necessary level of protection is provided, depending on the conditions in the third country, there

may be a need for additional measures are taken to ensure that the necessary level of protection is provided.[3] Such supplementary measures can be both technical, organizational and contractual.[4]

It is thus necessary to – in each individual case – examine whether the legislation in the third country ensures the necessary level of protection of the personal data that is transferred on the basis of the standard contract, and if necessary to take supplementary measures in addition to the standard contract.[5]

The Court of Justice of the European Union has also assessed whether selected legislation in the USA – Foreign Intelligence Surveillance Act (FISA) section 702 and Executive Order 12 333 (E.O. 12 333) – allows US public authorities to interfere with the rights of data subjects to the extent of a way that does not meet the minimum requirements of EU law.

FISA Section 702 (FISA 702) authorizes the US government to obtain information on persons who are not US citizens, etc. ("non-U.S. persons") and who can reasonably be expected to be outside the United States, for the purpose of collecting foreign intelligence information ("foreign intelligence information"). This is done by issuing directives to "electronic communications service providers" to hand over or arrange for the handing over of personal data that is sent to or received from a "selector", as part of this communication is also passed on to law enforcement authorities.[6]

With respect to E.O. 12333, this legal basis allows law enforcement agencies to access information that is “in transit” to the United States by accessing undersea cables, and to collect and store that information before it reaches the United States and becomes subject to FISA regulations. [7]

The European Court of Justice then ruled that neither FISA section 702 nor E.O. 12 333, together with Presidential Policy Directive-28 (PPD-28), meets the proportionality requirements of EU law with the consequence that surveillance programs based on these provisions cannot be considered to be limited to what is strictly necessary. The Court further held that FISA 702 or E.O. 12 333, taken together with PDD-28, do not provide registered rights that are enforceable against the US authorities in the courts.[8]

In its assessment of whether there are conditions in the USA that prevent the standard contract, which is used as a basis for transfer, from being a sufficient means of ensuring a level of protection that essentially corresponds to the level within the EU/EEA, Helsingør Municipality has stated, that it is likely that Google LLC should be considered an "electronic communications service provider", as this term is defined in 50 U.S.C. § 1881(b)(4).

It is the Danish Data Protection Authority's assessment that Google LLC - when providing the service (support, etc.) that gives

rise to the transfer of personal data to it - must be considered an "electronic communications service provider" and thus may be subject to directives from law enforcement authorities under FISA 702.

Helsingør Municipality has also stated that there is a high probability that information available to Google LLC per se cannot be accessed under FISA 702, as the personal data is not transferred by Google LLC, but to Google LLC for the purpose of providing support . Helsingør Municipality has stated below that it is thus an electronic communication to a "U.S. person", therefore, in light of the limitations found in FISA 702, law enforcement agencies are precluded from obtaining this information.

The municipality has also stated that the personal data that is transferred to Google LLC does not constitute personal data about "U.S. person's", and that law enforcement agencies are also barred from collecting the information under FISA 702 for this reason as well.

After a review of the legal restrictions on the collection of information under FISA 702[9], the Danish Data Protection Authority is of the opinion that the restrictions are aimed at preventing the collection - both directly and indirectly - of information about US persons, including companies, when such persons are the goal of the collection.

Thus, in the Data Protection Authority's opinion, the restrictions do not apply if and to the extent that Danish citizens or Helsingør Municipality as a whole become the subject of the collection of information in accordance with FISA 702.

Furthermore, the Danish Data Protection Authority is of the opinion that, according to its purpose, FISA 702 constitutes a legal basis for US law enforcement authorities to obtain information about foreign persons who can reasonably be expected to be outside the US, for the purpose of collecting foreign intelligence information.

Against this background, it is the Danish Data Protection Authority's assessment that the personal data transferred to Google LLC will be able to be obtained by American law enforcement authorities. The Danish Data Protection Authority has hereby emphasized that Google LLC must be considered an "electronic communications service provider", and that the personal data transferred to Google LLC relates to the municipality's school pupils and employees, i.e. Danish citizens.

It is thus the Danish Data Protection Authority's assessment that the transfer of the information in question is covered by conditions in the USA which prevent the standard contract, which is used as a basis for transfer, from being a sufficient means of ensuring a level of protection that essentially corresponds to the level within the EU/ EEA. Helsingør Municipality is thus obliged to ensure that supplementary measures are established that can bring the level of protection up to the required level.

The Norwegian Data Protection Authority notes below that contractual and organizational supplementary measures will

generally not counter access to or collection of personal data by US law enforcement authorities for surveillance purposes. It will therefore be necessary to take additional technical measures.

Helsingør Municipality has stated that the personal data is encrypted both in transit and at rest when the information is transferred and processed by Google LLC. However, the municipality has also stated that Google LLC can access the information in plain text.

It is the Danish Data Protection Authority's assessment that encryption can be an effective supplementary measure that is suitable to supplement the EU Commission's standard contract and, overall, bring the level of protection in a third country up to the required European level.

However, the Danish Data Protection Authority finds that the encryption in the present case is not suitable to address the conditions in the USA which prevent the standard contract from being a sufficient means of ensuring the effective protection of the transferred personal data.

The Danish Data Protection Authority has hereby emphasized that the collection of personal data by American law enforcement authorities in accordance with FISA 702 takes place by issuing directives to "electronic communication service providers" and thus presupposes their assistance, and that the transferred personal data under these circumstances can be obtained under FISA 702, as Google LLC has access to the information in plain text.

The Danish Data Protection Authority then finds that personal data that the Municipality of Helsingør has instructed Google Cloud EMEA Limited to transfer to the USA is not ensured a level of protection that essentially corresponds to the level of protection in the EU/EEA, and that the Municipality of Helsingør has not taken the necessary supplementary measures to bring the level of protection up to the required level.

The Danish Data Protection Authority therefore finds that the transfer of personal data that Helsingør Municipality has instructed Google Cloud EMEA Limited to carry out does not take place in accordance with Article 44 of the Data Protection Regulation, cf. Article 46, subsection 1, letter c.

4.7. Summary

In view of the announced order of 10 September 2021, and the announced processing restriction of the same date, and after a review of Helsingør Municipality's risk assessment and the municipality's other documentation, the Data Protection Authority finds that there are grounds for notifying Helsingør Municipality of a ban on processing personal data using Google

Chromebooks and Workspace for Education. The ban applies until the Municipality of Helsingør has brought the processing activity in accordance with the data protection regulation as stated in this decision, as well as prepared adequate documentation for this.

In addition, 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 is suspended until Helsingør Municipality can demonstrate that the rules in Chapter V of the data protection regulation have been observed.

The ban and suspension will take effect immediately, but Helsingør Municipality is granted a deadline of 3 August 2022 to withdraw and terminate users and rights, as well as delete already transferred information.

The bans are announced in accordance with the data protection regulation, article 58, subsection 2, letters f and j.

Violation of a ban announced by the Danish Data Protection Authority is punishable pursuant to section 41, subsection of the Data Protection Act. 2, no. 4, with a fine or imprisonment of up to 6 months, cf. section 41, subsection 1.

The Danish Data Protection Authority finally finds grounds for expressing serious criticism that Helsingør Municipality's processing of personal data has 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.

4.8. Choice of corrective measures

When choosing a corrective measure, the Danish Data Protection Authority has placed emphasis on bringing the illegal situation to an end quickly. In addition, the Data Protection Authority has, in mitigation, given weight to the fact that Helsingør Municipality - in all phases of the processing of the case - has contributed positively and responsibly to create the necessary documentation and clarity about the processing, just as it has given particular weight to the transfer of personal data in question to The USA was previously subject to an adequacy assessment, cf. the regulation's Article 45, which lapsed.

5. Concluding remarks

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

[1] Judgment of the European Court of Justice of 16 July 2020 in case C-311/18, Schrems II, paragraphs 101 and 105.

[2] Judgment of the European Court of Justice of 16 July 2020 in case C-311/18, Schrems II, paragraph 126

[3] Ibid., paragraph 133.

[4] European Data Protection Board Recommendations 01/2020 on supplementary measures, section 52.

[5] Judgment of the European Court of Justice of 16 July 2020 in case C-311/18, Schrems II, paragraph 134

[6] Ibid., paragraph 61.

[7] Ibid., paragraph 63.

[8] Judgment of the European Court of Justice of 16 July 2020 in case C-311/18, Schrems II, paragraphs 181, 182 and 184.

[9] See U.S.C. 50 Section 1881a(b).