DATATILSYNET

14 July 2022

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

In a case concerning the use of Chromebooks in Helsingør Municipality, the Danish Data Protection Agency has expressed serious criticism and imposed a ban on transfers to third countries and on the use of Google Workspace.

Summary

The Danish Data Protection Agency has for some time been focusing on the use of Chromebooks and Google Workspace (formerly G Suite for Education) in local authorities. Their use is widespread nationwide, but specifically, the Danish Data Protection Agency has had a pending case involving Helsingør Municipality.

Accordingly, the Danish Data Protection Agency issued a decision in September 2021, in which Helsingør Municipality was, amongst other things, ordered to carry out a risk assessment of the municipality's processing of personal data in Danish primary and lower secondary schools through the use of Chromebooks and Workspace. Based on the documentation and assessment of the risk to data subjects prepared by Helsingør Municipality, the Danish Data Protection Agency has now concluded that the processing fails to meet the requirements of the GDPR on several points.

"Helsingør Municipality has done a great deal of thorough work to map out how personal data is used in Danish primary and lower secondary schools, but this also highlights the data protection issues that may arise from the ways in which large tech companies approach the task," says Allan Frank, an IT security specialist and lawyer at the Danish Data Protection Agency.

The Danish Data Protection Agency finds that the municipality has not assessed certain very specific risks relating to the data processor arrangement. Furthermore, it is apparent from the data processing agreement that information may be transferred to third countries in support situations without the necessary level of security.

In light of the decision from September 2021, the Danish Data Protection Agency has now issued a decision. It includes, amongst other things:

- A suspension of Helsingør Municipality's processing operations involving the transfer of information to third countries without the necessary level of protection

- A general ban on processing using Google Workspace until adequate documentation and a data protection impact assessment have been prepared, and until the processing operations have been brought into compliance with the Regulation

Serious criticism of the municipality's processing of personal data

The Danish Data Protection Agency points out that many of the conclusions in this decision are likely to apply to other local authorities using the same processing arrangements. The Danish Data Protection Agency therefore expects these local authorities to take appropriate action themselves in light of the decision – even though the Agency is currently finalising a number of cases concerning other local authorities.

Decision

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

On 10 September 2021, the Danish Data Protection Agency issued a decision regarding the personal data breach. The Danish Data Protection Agency found, amongst other things, 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 carried out in accordance with Article 5(2) of the General Data Protection Regulation, cf. Article 5(1)(c) and (f), and Article 5(1)(a), cf. Article 6(1), as well as Article 32(1), Article 33(1) and Article 35(1).

Furthermore, the Danish Data Protection Agency found that there were grounds for issuing an order to Helsingør Municipality to bring its processing of personal data through the use of Google Chromebooks into compliance with the General Data Protection Regulation. This was to be achieved by Helsingør Municipality carrying out a risk assessment of the processing activity, reflecting the flows of personal data involved in the processing. The risk assessment was to address, on the one hand, the necessary options for configuring the product and, on the other, the scope of the legal basis in the Primary and Lower Secondary Education Act for the use of Chromebooks required of pupils by the municipality. If the risk to the rights and freedoms of data subjects was assessed as high, the municipality was also required, as part of the order, to carry out an impact assessment.

The order was issued pursuant to Article 58(2)(d) of the General Data Protection Regulation.

The Danish Data Protection Agency further found that there were grounds for issuing a warning to Helsingør Municipality that the use of Google G Suite add-on programmes without carrying out a data protection impact assessment, cf. Article 35(1) of the Regulation, would likely be in breach of the General Data Protection Regulation.

Finally, the Danish Data Protection Agency found that there were grounds for imposing a temporary limitation on the processing activity on Helsingør Municipality if the risk assessments which the municipality was ordered to carry out revealed a high risk to the rights and freedoms of data subjects, and the municipality had not reduced these risks to a level lower than high by the expiry of the deadline set in the order. The restriction meant that the processing of personal data involving a high risk to the rights and freedoms of data subjects was not permitted until the risks had been reduced to a level lower than high.

Following the Danish Data Protection Agency's decision of 10 September 2021, Helsingør Municipality submitted, by letter dated 10 November 2021, its risk assessment concerning the

use of Google Chromebooks and G Suite for Education, and the municipality has also submitted further documentation to demonstrate the lawfulness of the processing activity. Furthermore, on 9 December 2021 – in response to the Danish Data Protection Agency's request of 2 December 2021 – the municipality submitted further information on the case.

1. Decision

Following a review of Helsingør Municipality's risk assessment and the municipality's documentation in general, the Danish Data Protection Agency finds that there are grounds to issue Helsingør Municipality with a prohibition against processing personal data through the use of Google Chromebooks and Workspace for Education. The prohibition shall remain in force until Helsingør Municipality has brought the processing activity into compliance with the General Data Protection Regulation as set out in this decision, and has prepared adequate documentation to that effect.

In addition, any transfer of personal data to the USA, which Helsingør Municipality has instructed Google Cloud EMEA Limited to carry out in its capacity as processor for the municipality, is suspended until Helsingør Municipality can demonstrate that the rules in Chapter V of the General Data Protection Regulation have been complied with.

The prohibition and suspension take effect immediately, but Helsingør Municipality is granted a deadline of 3 August 2022 to revoke and deactivate users and rights, and to have data already transferred deleted.

The prohibitions are imposed pursuant to Article 58(2)(f) and (j) of the General Data Protection Regulation.

A breach of a prohibition issued by the Danish Data Protection Agency is punishable under Section 41(2), no. 4 of the Data Protection Act by a fine or imprisonment for up to six months, cf. Section 41(1).

Finally, the Danish Data Protection Agency finds grounds to express serious criticism of the fact that Helsingør Municipality's processing of personal data has not been carried out in accordance with Article 5(2) of the General Data Protection Regulation, cf. Article 5(1)(a), Article 24, cf. Article 28(1), Article 35(1), and Article 44, cf. Article 46(1).

2. Statement of the case

On 11 December 2019, a member of the public lodged a complaint with the Danish Data Protection Agency regarding Helsingør Municipality's processing of personal data.

In a letter dated 6 January 2020, Helsingør Municipality confirmed that, in 2019, a parent had complained to the municipality that his child – without his knowledge – had had a YouTube account created, as a result of which the child's name could be made public on YouTube.

Helsingør Municipality further stated that it considered it unlikely that the incident had posed a risk to the rights and freedoms of the data subjects and had therefore not given rise to a requirement to report a personal data breach to the Danish Data Protection Agency, cf. Article 33(1) of the General Data Protection Regulation.

On 29 January 2020, Helsingør Municipality reported the incident to the Danish Data Protection Agency as a personal data breach. At the same time, a number of other local authorities

made similar reports, which is why the Danish Data Protection Agency dealt with the cases collectively; by letter dated 11 March 2020, the Agency requested a statement from the local authorities concerned.

On 10 September 2021, the Danish Data Protection Agency issued a decision concerning the personal data breach in question, which Helsingør Municipality had reported to the Agency. The Danish Data Protection Agency's decision of 10 September 2021 is reproduced above in section 1, and the decision in its entirety is attached as **an annex**.

Following the Danish Data Protection Agency's decision of 10 September 2021, Helsingør Municipality submitted, by letter dated 10 November 2021, its risk assessment concerning the use of Google Chromebooks and G Suite for Education, and the municipality has also submitted further documentation to substantiate the lawfulness of the processing activity. Furthermore, on 9 December 2021 – in response to the Danish Data Protection Agency's request of 2 December 2021 – the municipality submitted further information on the matter.

3. Helsingør Municipality's statement

3.1. Conducting a risk assessment, including, where appropriate, a data protection impact assessment

On 10 November 2021, Helsingør Municipality submitted the municipality's risk assessment regarding 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 Agency that the municipality does not use Google Workspace's additional services and has, on that basis, concluded that it is not obliged to carry out a data protection impact assessment.

3.2. Processing of personal data for other purposes

The risk assessment identifies, amongst the risks that Helsingør Municipality has identified in connection with the use of 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 may use personal data relating to teachers and pupils for marketing or other purposes for which Helsingør Municipality, as the controller, does not wish personal data to be processed. In particular, contact details, IP addresses and digital traces (general information) are relevant in this context. It should be noted that this concerns personal data relating to pupils, who enjoy special protection under data protection rules; therefore, access to and the processing of personal data relating to pupils constitute a further element in relation to the risk assessment."

Regarding the likelihood of this risk materialising, the following applies:

"The municipality uses the Google Workspace for Education Standard product, under which the municipality is assured, by virtue of the data processing agreement, that data will not be 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, in which 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, Gmail, Chat, Chrome Sync, Groups, Meet, Vault, Reminders, Jamboard, Calendar, Keep (sticky notes), Tasks, Sites)

Additional services from Google are subject to different terms in the data processing agreement, which means that the local authority cannot instruct Google on how personal data may be used. The local authority has therefore disabled the use of Additional Services.

Conclusion

In light of the measures implemented as described above, Helsingør Municipality assesses that the likelihood of the risk materialising is low. However, it cannot be completely ruled out that Google may breach its contractual obligations and nevertheless use personal data for marketing or other unintended purposes for which Helsingør Municipality has not provided instructions, as set out in the data processing agreement."

3.3. Transfer of personal data to third countries

The risk assessment identifies the risk of transfers to third countries as a further risk identified by Helsingør Municipality in connection with the use of Google Chromebooks and Workspace for Education.

The risk is described as follows:

"There is a risk that personal data relating to pupils and teachers (generally ordinary personal data, but it cannot be ruled out that sensitive personal data may also be included) may be transferred to unsafe third countries without a necessary legal basis for the transfer and without ensuring that the third country in question guarantees data protection rights equivalent to those in other EU countries."

Regarding the likelihood of this risk materialising, the following applies:

"As the controller responsible for the processing of pupils' personal data, Helsingør Municipality has implemented the following relevant mitigating measures with a view to reducing the likelihood of the described risk becoming a reality:

The European Commission's standard contractual clauses have been adopted (basis for transfer), as there is a risk of access from the US via support services. As a further basis for this (supplementary measures), a separate Transfer Impact Assessment (TIA) has been drawn up in accordance with the requirements of the Danish Data Protection Agency and the EDPB. Reference is made to the TIA in question.

It should also be noted that Helsingør Municipality has opted for a solution whereby, as a clear starting point, data is located solely within the EU in the relevant data centres. It is therefore solely the risk of support access from an unsafe third country that could 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

In light of the measures implemented as outlined above, Helsingør Municipality assesses that the likelihood of this risk materialising is low."

Furthermore, Helsingør Municipality has submitted its documentation demonstrating compliance with Chapter V of the General Data Protection Regulation (GDPR) in relation to the use of Google Workspace for Education, in the form of the municipality's 'Transfer Impact Assessment' (hereinafter 'TIA').

It appears from this that Helsingør Municipality uses Google Cloud EMEA Limited as a processor in relation to its use of Google Chromebooks and Workspace for Education. The municipality has, through settings in Google Workspace for Education, ensured that personal data is stored solely in data centres 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 for support purposes. The transfer takes place on the basis of the European Commission's standard contractual clauses.

Finally, the following is stated in 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 known as Workspace), which Helsingør Municipality uses for the purpose of educating pupils as part of its statutory obligation as a local public authority to provide education. Helsingør Municipality considers that this obligation is best fulfilled with Google as the provider of the above services, and the Danish Data Protection Agency has accepted this premise in accordance with the relevant provisions of the Danish Primary and Lower Secondary Education Act.

In order for Helsingør Municipality to use the aforementioned services and products offered by Google, it is a requirement that Helsingør Municipality transfers the personal data relating to the data subjects set out in sections 1.9–1.10 below to Google's cloud. The purpose of the transfer is therefore to store the personal data in the data centres (cloud), ensure a high level of security for the personal data, and to receive management and support from Google."

As far as the Danish Data Protection Agency understands, Helsingør Municipality has, in the TIA, assessed whether the basis for transfer to the USA in the form of the standard contractual clauses 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 standard contractual clauses entered into.

Section 2.4 of the TIA 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 Kommunes 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 EU law as stated in the Schrems II judgement 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, and in some cases Google object to producing any information at all. Google will share the number and types of requests received in the Transparency Report.
B) When Google receive 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 organisation, 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 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 the US require the 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 believe 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:

i. It is statistically improbable that Helsingør Kommune will be the target of a request regarding the use of GCP and G-Suite (now named Workspace).
ii. 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.
iii. The number of NSL requests is so low than it is statistically without importance.
iv. 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 is also stated in section 3.4 of the TIA that the personal data transferred to Google LLC in the USA will be accessible 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 Minicipality'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 center, it serves as a mitigating factor to meet regulatory or compliance obligations, i.e. in accordance with the guidelines from the EDPB."

Furthermore, section 3.5 of the TIA concerning the established basis for transfer states:

"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 obligated as processor to comply with comply with the obligations applicable to it under European Data Protection Law with respect to the processing of Helsingør Municipality'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, clause 4.1.1 of the TIA states, with regard to legislation and/or practice in the USA that affects 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 a 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 centres 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 is stated below that Helsingør Municipality has assessed the likelihood that the above assessment is accurate as 40 per cent.

Following Helsingør Municipality's letter of 10 November 2021, including its annexes, the Danish Data Protection Agency requested further information from the municipality on 2 December 2021. The Danish Data Protection Agency stated, amongst other things, that any transfers of personal data to the USA as part of support services were – in the Agency's view – intentional, notwithstanding the fact that the municipality had assessed this as a risk regarding support access from the USA.

The Danish Data Protection Agency requested, amongst other things, that Helsingør Municipality provide a copy of the municipality's legal basis for the transfer, any amendments to the instructions and the data processing agreement with Google, as well as an overview of any supplementary measures that the municipality might have deemed necessary.

In a letter dated 9 December 2021 – clarifying the aforementioned risk – Helsingør Municipality stated the following:

"The potential transfer to Google – and the associated risk – is linked to Google's setup. In other words, even though the municipality has opted for an EU cloud, Google has secured the right in the data processing agreement to potentially obtain support from third countries. This is also the reason why Google has established a basis for data transfers in accordance with the new SCCs (from June 2021), which the municipality takes into account in its risk assessment.

More generally, with regard to the risk associated specifically with support, the following considerations may be taken into account: In very specific support situations involving an unsafe third country, there will be a very limited window of opportunity during which the support provider may potentially gain access to personal data in plain text. It is highly unlikely that, during that limited window, the support provider would be obliged by the government [of the unsafe third country] to disclose the personal data.

The local authority further notes that it is apparent from the TIA prepared that the local authority has assessed that the use of Google Workspace for Education is necessary to fulfil the local authority's duties under the Primary and Lower Secondary Education Act, that the option of support from third countries cannot be ruled out when Google is the processor, and that the local authority has therefore assessed the risks associated with using Google.

As stated, the legal basis for the transfer is the new SCCs (from June 2021)."

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

"There are different 'data sources' in relation to the risk assessment and the TIA. The risk assessment is based, on the one hand, on the fact that the data processing agreement sets out in detail the relationship between the parties – i.e. that Google is the processor for the municipality and that Google reserves the right to provide support from third countries – and, on the other hand, on the fact that the municipality has ensured that the service is provided from an EU cloud.

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

Furthermore, Helsingør Municipality has provided the following information regarding its assessments set out in the TIA:

"The assessments in the TIA regarding the likelihood that the individual legal arguments hold up are estimates. In this context, it is the municipality's assessment that the probabilities stated are conservative, i.e. that the municipality has given the benefit of the doubt to the rights and freedoms of data subjects. If the Danish Data Protection Agency has a different, reasoned assessment of the likelihood that the individual arguments hold water, the municipality would be happy to hear about it. It should also be noted, for the sake of good order, that the calculated overall risk – based, amongst other things, on these arguments, the circumstances surrounding the possible transfer, published statistics from Google, established practice and the mitigating measures – is quite low. The local authority further undertakes to continuously monitor and evaluate the likelihood that these arguments hold true.

The lawfulness of the use of Google Workspace for Education is therefore, in these circumstances, not dependent on whether the assessment of the likelihood that a single argument holds true can be challenged with well-founded arguments."

Finally, Helsingør Municipality has submitted a large amount of documentation concerning the data processor arrangement 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. Reasons for the Danish Data Protection Agency's decision

In general, it is the Danish Data Protection Agency's view that a controller using a processor – for all processing operations – must comply with, and be able to demonstrate compliance with, the General Data Protection Regulation and the Data Protection Act, regardless of where in the data processing chain the processing takes place.

This follows from Article 5(2) of the General Data Protection Regulation, which states that the controller is responsible for and must be able to demonstrate compliance with paragraph 1.

This means, amongst other things, that the controller is responsible for and must be able to demonstrate that personal data is processed lawfully, fairly and in a transparent manner, cf. Article 5(1)(a).

Furthermore, Article 24(1) of the Regulation states that the controller must implement appropriate technical and organisational measures to ensure, and to be able to demonstrate, that processing is carried out in accordance with this Regulation. This must be done taking into account the nature, scope, context and purposes of the processing in question, as well as the risks of varying likelihood and severity to the rights and freedoms of natural persons, and the measures must be reviewed and updated where necessary.

In this decision, the Danish Data Protection Agency has considered solely whether – and to what extent – Helsingør Municipality, as the controller, processes personal data in accordance with data protection rules. The Danish Data Protection Agency's jurisdiction derives from Section 27 of the Data Protection Act and Chapters VI and VII of the General Data Protection Regulation, including Article 55(2) of the Regulation.

4.1. Use of Google Chromebooks and Google Workspace for Education

It follows from Section 2(1) of the Primary and Lower Secondary Education Act that the local council is responsible for primary and lower secondary schools.

For primary and lower secondary education, it follows from Section 18(1) and Section 19 of the Act that the organisation of teaching – including the choice of teaching and working methods, approaches, teaching materials and subject content, as well as the funding thereof – in all subjects must meet the objectives of primary and lower secondary education, subject objectives and topics, and be varied so as to meet the needs and abilities of each individual pupil.

It is the Danish Data Protection Agency's view that decisions regarding the use of IT in teaching, including which brand and software are to be used, fall within this scope.

The Danish Data Protection Agency notes, in this regard, that the data protection rules are technology-neutral, and the Agency can only assess situations where the processing of personal data takes place, cf. Article 2(1) of the General Data Protection Regulation.

Whilst the Primary and Lower Secondary Education Act – in the Danish Data Protection Agency's view – confers on the local authority the power to decide whether – and, if so, which – IT equipment is to be used in teaching, such use must continue to take place within the framework of the General Data Protection Regulation and the Data Protection Act.

The rights of children and young people enjoy special protection under data protection rules. It is the Danish Data Protection Agency's view that this consideration forms part of the assessment of which processing operations may be carried out on the basis of the legal authority granted to individual local authorities by the Primary and Lower Secondary Education Act.

As is also evident from the Danish Data Protection Agency's decision of 10 September 2021, it is the Agency's view that Helsingør Municipality may determine which tools are used in the municipality's primary schools, cf. Article 6(1)(e) of the General Data Protection Regulation. This also applies to the registration of individual pupils as users of such a system.

However, it remains an essential prerequisite that the General 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 Agency generally considers that Helsingør Municipality's risk assessment regarding the use of Google Chromebooks and Workspace for Education addresses the most significant scenarios and threats.

However, it is the Danish Data Protection Agency's view that the use of new, complex technology, including software – particularly in the field of education, where the data subjects are children and young people – normally entails a high risk to the rights and freedoms of these pupils.

In this specific case, where it is common knowledge that the technologies used to deliver and support the chosen service – Google Chromebooks and Workspace for Education – are also used to deliver other parts of Google's product range, and that these are used for data collection, targeted marketing and the sale of such data. Such circumstances must therefore be taken into account in the assessment of the risks to the rights and freedoms of data subjects arising from the use of Google Workspace for Education.

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

It is the Danish Data Protection Agency's view that carrying out a specific risk assessment and impact assessment – prior to the distribution of IT equipment to pupils and the processing of pupils' data – is a prerequisite for establishing and maintaining an appropriate level of security. This is because an appropriate level of security must be assessed in the light of the risks, including the consequences, that the processing of pupils' personal data may have for the individuals concerned. The Danish Data Protection Agency notes that several of the aforementioned failures to comply with data protection rules could have been avoided had Helsingør Municipality assessed the risks associated with the processing and taken appropriate measures in light of those risks.

On the basis of the above, the Danish Data Protection Agency finds that Helsingør Municipality **– (i) by failing to** include in its risk assessment the risk scenarios that may arise as a result of the data processor arrangement and the system choices made, **(ii) by failing to** carry out sufficient testing of the scope and functioning of the selected hardware and the software used, and **(iii) by** failing to document how the municipality controls Google's access to personal data, including in particular during normal use of the Google Chromebook operating system and Google Workspace's interaction with Google's backend in relation to the possibilities for separating personal data that may arise under the data processor agreement – has failed to demonstrate that personal data is processed lawfully, fairly and in a transparent manner in relation to the data subject, cf. Article 5(2) of the Data Protection Act, cf. Article 5(1)(a).

4.3. Use of data for other purposes

It is the Danish Data Protection Agency's view that Helsingør Municipality's processing of personal data under the Primary and Lower Secondary Education Act, cf. Article 6(1)(e) of the Regulation, does not cover situations where personal data is processed for purposes other than those provided for in the Primary and Lower Secondary Education Act. Consequently, the data may not lawfully be disclosed to other controllers for their own purposes where such purposes are not provided for in the Primary and Lower Secondary Education Act. This also includes the processing of personal data that may occur through pupils' use of the equipment and software, including metadata used for marketing and profiling, regardless of whether the data is used for direct marketing towards the individual pupil or indirectly as part of a group (class, year group, school, etc.).

The Danish Data Protection Agency assumes that Helsingør Municipality does not use Google Workspace for Education's add-on products.

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

The Danish Data Protection Agency assumes that Helsingør Municipality, as the controller, has assessed that "it cannot be entirely ruled out that Google may breach its contractual obligations and nevertheless use personal data for marketing or other unintended purposes for which Helsingør Municipality has not provided instructions, in accordance with the data processing agreement."

The Danish Data Protection Agency further finds that Helsingør Municipality also processes special categories of personal data, as referred to in Article 9 of the Regulation, through its use of Google Workspace for Education.

In this connection, the Danish Data Protection Agency wishes to emphasise in general that a controller – pursuant to Article 28(1) of the General Data Protection Regulation – must only use processors who can provide the necessary guarantees that they will comply with data protection rules when processing the data on behalf of the controller.

This means that a belief on the part of the controller that the chosen processor will act in breach of the data processing agreement entered into – in itself – means that the controller cannot use that processor, cf. Article 28(1) of the Regulation.

However, the Danish Data Protection Agency has taken the view that, in its assessment of this risk, Helsingør Municipality regards the risk of the processor acting in breach of the data processing agreement as merely hypothetical rather than definitively foreseeable.

The Danish Data Protection Agency finds that Helsingør Municipality – in its assessment of this risk – has not demonstrated that, in this situation, it is using a processor capable of providing the necessary guarantees that the processor will comply with the requirements of the General Data Protection Regulation, see Article 24 of the Regulation, in conjunction with Article 28(1).

The Danish Data Protection Agency has placed particular emphasis on the fact that there would be a significant loss of rights for data subjects if the risk in question were to materialise, and that the municipality has not, in its risk assessment, set out any genuinely effective

technical and organisational measures to mitigate this risk. In this regard, the Danish Data Protection Agency considers that Helsingør Municipality's reference to its confidence that the supplier generally complies with the agreement does not constitute a sufficient reduction of this risk.

The Danish Data Protection Agency further notes that any risk entailing a high impact on the rights and freedoms of data subjects – even where the probability of the risk materialising is relatively low – is likely to entail a high risk to the rights of data subjects, which triggers the obligation to carry out a data protection impact assessment, cf. Article 35(1) of the Regulation.

In view of this – and of Helsingør Municipality's own assessment that it cannot be ruled out that the processor will act in breach of the data processing agreement – it is the Danish Data Protection Agency's view that the situation triggers the obligation to carry out a data protection impact assessment, in accordance with Article 35(1) of the Regulation.

Against this background – and given that Helsingør Municipality has stated that it has not carried out a data protection impact assessment – the Danish Data Protection Agency finds that Helsingør Municipality's processing of personal data has not been carried out in accordance with Article 35(1) of the Regulation.

4.4. Transfer of personal data to third countries
4.5. Transfer of personal data via the cloud infrastructure

The Danish Data Protection Agency has, as a preliminary point, 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 "as a clear starting point, data is located solely within the EU in the relevant data centres. It is therefore solely the risk of support access from an unsafe third country that could lead to access from an unsafe third country."

Helsingør Municipality's contractual basis with Google, which governs the processing activity, includes, amongst other things, the "Data Processing Amendment to Google Workspace and/or Complementary Product Agreement" (contractual amendment), dated 24 September 2021.

The amendment states, amongst other things, the 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. […]

11. Sub-processors

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 11.2 of the Addendum refers to a list of sub-processors used for the provision of Google Workspace for Education. The list sets out a large number of sub-processors used to provide technical support, which are located both within the EU and in third countries, including third countries where the European Commission has not adopted a decision on the level of protection afforded by those countries, cf. Article 45.

The overview also lists a large number of Google's subsidiaries that are used for limited activities in connection with, amongst other things, Google Workspace, and which are also located both within and outside the EU/EEA.

In this decision, the Danish Data Protection Agency has not taken a position on the extent to which Helsingør Municipality, by using Google Workspace for Education – in addition to the USA, see further details below in section 4.6 – transfers personal data to other third countries, notwithstanding that the data is 'stored' within the EU/EEA.

However, the Danish Data Protection Agency must recommend that Helsingør Municipality – inter alia, by reviewing the Google Workspace 'Service Specific Terms' referred to in clause 10.1 of the addendum to the agreement – ensures that the data, as part of processing other than 'storage' – for example, as part of general service and support for the underlying cloud infrastructure, etc. – is not transferred to third countries, unless Helsingør Municipality instructs the processor to do so and provides a valid legal basis for the transfer.

It is the Danish Data Protection Agency's view that the controller must provide a valid legal basis for transfer to all third countries to which personal data may be transferred as part of the provision of a service under the contractual framework, including in connection with service and support.

4.6. Transfer of personal data to the USA

Firstly, the Danish Data Protection Agency notes that – in its view – this constitutes an intended and authorised transfer to the USA on the part of Helsingør Municipality as a result of the agreed provision for support – in or from the USA – with access to personal data.

The rules on transfers to third countries, including the possible legal bases for such transfers, are set out in Chapter V of the General Data Protection Regulation.

The main rule governing the transfer of personal data to third countries is set out in the general principle in Article 44 of the General Data Protection Regulation. This states that:

"Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined."

Any transfer of personal data may therefore only take place if the conditions set out in Chapter V of the Regulation are met.

The Danish Data Protection Agency interprets Article 44 of the Regulation as an obligation incumbent on both the controller and the processor. Both parties are therefore obliged to ensure that a legal basis for the transfer is established which is effective in the light of all the circumstances of the transfer. This also applies in cases where, in practice, it is the processor who has entered into a standard contractual clause pursuant to Article 46(2)(c) of the Regulation with any sub-processors in third countries. In such cases, the obligation on the controller consists, in practice, of ensuring – and is able to demonstrate to the Danish Data Protection Agency – that the processor has established the necessary legal basis for the transfer, and that this legal basis is effective in light of all the circumstances of the transfer, including the implementation of supplementary measures where necessary.

It is further the Danish Data Protection Agency's view that – subject to the exceptions in Article 49 of the Regulation – the wording of Article 44, which states that any transfer of personal data may only take place if the conditions set out in Chapter V are met, read in conjunction with the principle that the level of protection ensured by the General Data Protection Regulation must not be undermined, must be understood to mean that every transfer must be subject to the necessary safeguards. It is therefore not sufficient that almost all transfers, or a percentage of transfers, benefit from the protection provided for in the General Data Protection Regulation, unless this is authorised by the Regulation.

One way of establishing a valid basis for transfer under Chapter V is to enter into standard contractual clauses adopted by the European Commission with the organisation in the third country to which the data is transferred, cf. Article 46(1)(c) of the Regulation.

It is apparent from the case that Helsingør Municipality has instructed its processor – Google Cloud EMEA Limited in Ireland – to transfer personal data to a sub-processor – Google LLC – in the USA. The transfer takes place on the basis of an EU Commission standard contractual clause between Google Cloud EMEA Limited and Google LLC in the US. This standard contractual clause 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 Court of Justice of the European Union clarified that the use of the European Commission's standard contractual clauses presupposes that a level of protection for personal data in the third country concerned can be ensured which is essentially equivalent to the level of protection within the EU/EEA.[1]

The Court of Justice further noted that there may be situations where the European Commission's standard contractual clauses do not constitute "a sufficient means of ensuring, in practice, the effective protection of personal data transferred to the third country in question. This is particularly the case where the legislation of that third country permits its public authorities to interfere with the rights of data subjects in relation to that data."[2]

In such cases, where the standard contractual clause, given their nature, cannot provide guarantees going beyond the contractual obligation to ensure that the necessary level of protection is provided, it may, depending on the circumstances in the third country, be necessary to adopt supplementary measures to ensure that the necessary level of protection is provided.[3] Such supplementary measures may be technical, organisational or contractual in nature.[4]

It is therefore necessary – on a case-by-case basis – to assess whether the legislation of the third country ensures the necessary level of protection for the personal data transferred on the

basis of the standard contractual clauses and, where necessary, to adopt supplementary measures in addition to the standard contractual clauses.[5]

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

Section 702 of the FISA Act (FISA 702) authorises the US Government to collect information on persons who are not US citizens, etc. ("non-U.S. persons") and who can reasonably be expected to be located outside the United States, for the purpose of gathering foreign intelligence information ("foreign intelligence information"). This is done by issuing directives to 'electronic communications service providers' to disclose, or arrange for the disclosure of, personal data sent to or received from a 'selector', with part of this communication also being passed on to law enforcement authorities.[6]

With regard to E.O. 12333, this legal basis enables law enforcement authorities to access information in 'transit' to the US by tapping undersea cables, and to collect and store this information before it reaches the US and becomes subject to the provisions of FISA.[7]

The Court of Justice of the European Union subsequently ruled that neither FISA Section 702 nor E.O. 12333, read in conjunction with Presidential Policy Directive 28 (PPD-28), meet the EU Court's proportionality requirements, with the result that surveillance programmes based on these provisions cannot be regarded as being limited to what is strictly necessary. The Court further held that neither FISA Section 702 nor E.O. 12 333, read in conjunction with PPD-28, confers on data subjects rights that can be enforced against the US authorities in the courts.[8]

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

Similarly, the Danish Data Protection Agency assesses that Google LLC – in providing the service (support, etc.) that gives rise to the transfer of personal data to it – must be regarded as an "electronic communications service provider" and may therefore be subject to directives from law enforcement authorities pursuant to FISA 702.

The Municipality of Helsingør has further stated that there is a high probability that information accessible to Google LLC cannot, per se, be accessed under FISA Section 702, as the personal data is not transferred by Google LLC, but to Google LLC for the purpose of providing support. The Municipality of Helsingør has further stated that this therefore constitutes electronic communications to a 'U.S. person', and that, in light of the restrictions set out in FISA Section 702, law enforcement authorities are therefore precluded from obtaining this information. The municipality has further stated that the personal data transferred to Google LLC does not constitute personal data relating to 'U.S. persons', and that law enforcement authorities are therefore also barred from collecting the data under FISA 702.

Having reviewed the legal restrictions on the collection of information under FISA Section 702[9], it is the Danish Data Protection Agency's view that the restrictions are intended to

prevent the collection – both direct and indirect – of information concerning US persons, including companies, where such persons are the subject of the collection.

In the Danish Data Protection Agency's view, the restrictions therefore do not apply if, and to the extent that, Danish citizens or the Municipality of Helsingør as a whole become the subject of data collection under FISA 702.

Furthermore, it is the Danish Data Protection Agency's view that, by its very nature, FISA Section 702 constitutes a legal basis enabling US law enforcement authorities to obtain information on foreign individuals who can reasonably be expected to be located outside the US, for the purpose of gathering foreign intelligence.

Against this background, the Danish Data Protection Agency assesses that the personal data transferred to Google LLC may be accessed by US law enforcement authorities. In reaching this conclusion, the Danish Data Protection Agency has taken into account that Google LLC is to be regarded as an 'electronic communications service provider', and that the personal data transferred to Google LLC relates to the municipality's school pupils and staff, i.e. Danish citizens.

It is therefore the Danish Data Protection Agency's assessment that the transfer of the data in question is subject to circumstances in the US which prevent the standard contractual clauses used as the basis for the transfer from being a sufficient means of ensuring an adequate level of protection that is essentially equivalent to that within the EU/EEA. Helsingør Municipality is therefore obliged to ensure that supplementary measures are put in place to raise the level of protection to the required standard.

The Danish Data Protection Agency notes, in this regard, that supplementary contractual and organisational measures will generally not prevent access to or the collection of personal data by US law enforcement authorities for surveillance purposes. It will therefore be necessary to implement supplementary technical measures.

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

It is the Danish Data Protection Agency's assessment that encryption may be an effective supplementary measure, suitable for supplementing the European Commission's standard contractual clauses and, overall, bringing the level of protection in a third country up to the required European standard.

The Danish Data Protection Agency finds, however, that in the present case the encryption is not suitable for addressing the circumstances in the US which prevent the standard contractual clauses from being a sufficient means of ensuring the effective protection of the personal data transferred.

In this regard, the Danish Data Protection Agency has taken into account that the collection of personal data by US law enforcement authorities under FISA Section 702 takes place through the issuance of directives to 'electronic communication service providers' and thus requires their assistance, and that, under these circumstances, the personal data transferred may be obtained under FISA Section 702, as Google LLC has access to the data in plain text.

The Danish Data Protection Agency therefore finds that personal data which Helsingør Municipality has instructed Google Cloud EMEA Limited to transfer to the US is not afforded a level of protection that is essentially equivalent to the level of protection in the EU/EEA, and that Helsingør Municipality has not taken the necessary supplementary measures to bring the level of protection up to the required standard.

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

4.7. Summary

In view of the order issued on 10 September 2021, and the processing restriction issued on the same date, and following a review of Helsingør Municipality's risk assessment and the municipality's documentation in general, the Danish Data Protection Agency finds that there are grounds to issue a **prohibition** to Helsingør Municipality against processing personal data using Google Chromebooks and Workspace for Education. The prohibition shall remain in force until Helsingør Municipality has brought the processing activity into compliance with the General Data Protection Regulation as set out in this decision, and has prepared adequate documentation to that effect.

Furthermore, any transfer of personal data to the United States that Helsingør Municipality has instructed Google Cloud EMEA Limited to carry out in its capacity as processor for the municipality **is suspended** until Helsingør Municipality can demonstrate that the provisions of Chapter V of the General Data Protection Regulation have been complied with.

The prohibition and suspension take effect immediately, but Helsingør Municipality is granted a deadline of 3 August 2022 to revoke and terminate users and rights, and to have data already transferred deleted.

The prohibitions are imposed pursuant to Article 58(2)(f) and (j) of the General Data Protection Regulation.

A breach of a prohibition issued by the Danish Data Protection Agency is punishable under Section 41(2), no. 4 of the Data Protection Act by a fine or imprisonment for up to six months, cf. Section 41(1).

Finally, the Danish Data Protection Agency finds grounds to express **serious criticism** of the fact that Helsingør Municipality's processing of personal data has not been carried out in accordance with Article 5(2) of the General Data Protection Regulation, cf. Article 5(1)(a), Article 24, cf. Article 28(1), Article 35(1), and Article 44, cf. Article 46(1).

4.8. Selection of corrective measures

In selecting remedial measures, the Danish Data Protection Agency has placed emphasis on bringing the unlawful situation to an end swiftly. Furthermore, the Danish Data Protection Agency has, as a mitigating factor, taken into account that Helsingør Municipality – at all stages of the proceedings – cooperated positively and responsibly in providing the necessary documentation and clarity regarding the processing operations; particular weight has also been given to the fact that the transfers of personal data to the USA in question were previously subject to an adequacy assessment, cf. Article 45 of the Regulation, which has since lapsed.

5. Concluding remarks

The Danish Data Protection Agency notes that it is the responsibility of Helsingør Municipality to rectify and erase data in accordance with the decision. The municipality must therefore contact the parents of the data subjects concerned in order to carry out the rectifications, anonymisations or erasures of the personal data that the parents cannot themselves carry out in the systems where the pupils' personal data have been inadvertently published or disclosed.

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

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

[3] Ibid., paragraph 133.

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

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

[9] See 50 U.S.C. § 1881a(b).