DATATILSYNET

29 January 2026

The Danish Data Protection Agency issues serious criticism of 51 local authorities in the Chromebook case

The Danish Data Protection Agency has expressed serious criticism and, at the same time, warned the local authorities regarding their use of Google's products in Danish primary and lower secondary schools.

Summary

The Danish Data Protection Agency has issued a ruling in the so-called Chromebook case concerning 51 local authorities' use of Google's products for teaching in primary and lower secondary schools. The Agency has expressed serious criticism and warned the local authorities regarding their configuration of the programmes in question and their use of sub-processors outside the EU.

Among other things, the Danish Data Protection Agency has, as a follow-up to an opinion from the European Data Protection Board (EDPB) in October 2024 on the controller's obligations when using processors – as the final stage in the Authority's major investigation into a number of local authorities' use of Google Workspace for Education and Google Chrome for Education for teaching purposes in Danish primary and lower secondary schools – examined the local authorities' handling of the responsibilities associated with using Google as a processor.

The controller's responsibilities when using processors and sub-processors

The EDPB's opinion of October 2024 addresses, amongst other things, the extent to which the controller must be able to identify its processors, and the extent to which the controller must verify and document that any sub-processors are subject to the same data protection obligations as the primary processor.

The opinion also addresses the controller's documentation obligation in situations where a processor within the EU/EEA transfers personal data to a (sub-)processor in a third country – including subsequent onward transfers.

Focus on the use of sub-processors outside the EU

In this case, the Danish Data Protection Agency has focused on the use of sub-processors outside the EU employed by the local authorities' processor, Google. In this context, the Danish Data Protection Agency has examined the local authorities' considerations and documentation concerning the steps taken to make lawful the processing of personal data carried out by these sub-processors.

Key points of the Danish Data Protection Agency's decision

In its decision, the Danish Data Protection Agency has emphasised the following key points:

- The Danish Data Protection Agency has expressed serious criticism of the local authorities' processing of personal data through the use of Google's products for teaching in primary and lower secondary schools.
- The Danish Data Protection Agency has issued a warning to the local authorities that it is likely to be in breach of the General Data Protection Regulation if they have not configured their set-up of the programmes in question in accordance with the prerequisite and functional requirements set out by KL.
- The Danish Data Protection Agency has issued a warning to local authorities that it is likely to contravene the General Data Protection Regulation to engage a processor for the processing of personal data where further processing takes place in a third country, if a level of protection essentially equivalent to that in the EU/EEA cannot be ensured.
- Requirements for clear processing arrangements and ongoing compliance

Furthermore, the Danish Data Protection Agency states that, as a controller, one cannot lawfully use products that contain unclear processing arrangements.

The Danish Data Protection Agency also emphasises that the controller must have access to the necessary resources to ensure the lawful processing of personal data, including in situations where a chosen product or the contractual basis for the product changes.

Decision

Processing of personal data through the use of Google Chromebooks and Workspace for Education

The Danish Data Protection Agency hereby returns to the case in which, on 10 July 2024, the Agency informed KL that a final assessment of the sub-processor chain in connection with the municipalities' use of Google's products would be carried out on the basis of the European Data Protection Board's (hereinafter the EDPB) opinion on, amongst other things, the scope of the controller's obligation to document the processor's use of sub-processors.

In its decision, the Danish Data Protection Agency has confined itself solely to the assessment of the sub-processor chain in relation to the local authorities' use of Google Chromebooks and Workspace for Education.

On 28 January 2025, KL informed the Danish Data Protection Agency that KL represents the following 51 local authorities in the case (referred to in the case as 'the local authorities'):

- Albertslund Municipality
- Allerød Municipality
- Ballerup Municipality
- Brøndby Municipality
- Dragør Municipality
- Egedal Municipality
- Fanø Municipality
- Favrskov Municipality
- Faxe Municipality
- Fredericia Municipality
- Faaborg-Midtfyn Municipality
- Glostrup Municipality
- Greve Municipality
- Gribskov Municipality
- Haderslev Municipality
- Hedensted Municipality
- Helsingør Municipality

- Herlev Municipality
- Hjørring Municipality
- Holbæk Municipality
- Horsens Municipality
- Hvidovre Municipality
- Hørsholm Municipality
- Ishøj Municipality
- Jammerbugt Municipality
- Langeland Municipality
- Læsø Municipality
- Mariagerfjord Municipality
- Middelfart Municipality
- Nordfyn Municipality
- Næstved Municipality
- Odder Municipality
- Odense Municipality
- Randers Municipality
- Rebild Municipality
- Samsø Municipality
- Silkeborg Municipality
- Slagelse Municipality
- Solrød Municipality
- Sorø Municipality
- Svendborg Municipality
- Syddjurs Municipality
- Thisted Municipality
- Tønder Municipality
- Tårnby Municipality
- Vejen Municipality
- Vejle Municipality
- Vordingborg Municipality
- Vesthimmerland Municipality
- Aalborg Municipality
- Aarhus Municipality

1. Decision

The Danish Data Protection Agency finds that the processing of personal data by the 51 local authorities has not been carried out in accordance with Article 5(2) of the General Data Protection Regulation, cf. Article 5(1)(a) and Article 24, cf. Article 28(1) and (4).

Against this background, the Danish Data Protection Agency must, pursuant to Article 58(2)(b) of the General Data Protection Regulation, express serious criticism of the 51 local authorities.

Furthermore, pursuant to Article 58(2)(a) of the General Data Protection Regulation, the Danish Data Protection Agency must warn the 51 local authorities that it is likely to be in breach of Article 6(1) of the General Data Protection Regulation, cf. Article 6(3), if they have not configured the relevant software in accordance with the prerequisite and functional requirements specified by KL, both in connection with the previous cases in this series and as set out in this case.

Furthermore, pursuant to Article 58(2)(a) of the General Data Protection Regulation, the Danish Data Protection Agency must **warn** the 51 local authorities that it is likely to be in breach of Article 28(1) of the General Data Protection Regulation to engage a processor for the processing of personal data where such data is subject to further processing by a sub-processor in a third country where a level of protection essentially equivalent to that in the EU/EEA cannot be ensured.

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

2. Statement of the case

On 10 July 2024, the Danish Data Protection Agency wrote to KL regarding the so-called 'Chromebook case complex'. The letter stated that the Danish Data Protection Agency had decided to consult the EDPB to obtain an opinion on, amongst other things, the scope of documentation for data processing arrangements, including the relationship with sub-processors. Furthermore, the letter stated that the Danish Data Protection Agency would carry out a final assessment of the sub-processor chain in relation to the local authorities' use of Google's products once the EDPB's opinion was available.

On 4 April 2024, the Danish Data Protection Agency requested an opinion from the EDPB pursuant to Article 64(2) of the General Data Protection Regulation concerning, amongst other things, the scope of documentation for data processing arrangements, including the relationship with sub-processors.

The EDPB's opinion was published on 9 October 2024[1].

With reference to this and to the Danish Data Protection Agency's other comments in a letter dated 10 July 2024 concerning the requirements incumbent upon each municipality as a controller, the Agency asked KL on 27 January 2025 whether KL would coordinate a joint response on behalf of the municipalities.

On 28 January 2025, KL informed the Danish Data Protection Agency that it would continue to answer questions from the Agency on behalf of the municipalities concerned.

On 30 April 2025, the Danish Data Protection Agency sent a preliminary consultation to KL. The Danish Data Protection Agency requested a list of all processors used in the processing of personal data in connection with the municipalities' use of Google's products for educational purposes.

The Danish Data Protection Agency also requested that KL specify all the sub-processors used, the locations at which personal data is processed on behalf of the local authorities, and – to the extent necessary – documentation of the considerations the local authorities have made regarding the lawfulness of such processing.

In addition, the Danish Data Protection Agency requested that a corresponding list be attached for any disclosures to other independent controllers.

On 21 May 2025, KL submitted a response to the Danish Data Protection Agency's consultation. In addition, KL submitted a list of the 51 local authorities for which KL acts as a representative.

On the basis of the material submitted, the Danish Data Protection Agency requested on 4 June 2025 that KL provide a supplementary statement on the matter.

KL submitted a supplementary statement on the matter on 6 June 2025, in which it stated, amongst other things, that KL was still awaiting a response from Google to some outstanding questions relating to the sub-processors for Google Chrome Education Upgrade.

KL submitted its responses to the outstanding questions on 23 June 2025.

2.1. KL's comments

2.1.1. List of processors

KL has stated that Google Cloud EMEA Limited is the processor in connection with the local authorities' use of Google Workspace for Education and Google Chrome Education.

2.1.2. List of sub-processors

KL has submitted a number of annexes containing lists of Google's sub-processors for Google Workspace for Education and Chrome Education Upgrade. In the material submitted, Google's sub-processors are divided into 'Third Party Sub-processors' and 'Google Group Sub-processors' respectively.

2.1.2.1. Third-party sub-processors

According to KL, 'Third Party Subprocessors' do not have access to 'Customer Data' stored or processed by Google, unless the customer – which in this case would be the individual local authority – expressly chooses to share 'Customer Data' in connection with a support case.

KL has further stated that it has recommended that local authorities introduce organisational measures in the form of procedures to ensure that staff requesting support do not share personal data.

KL has stated that "Provided that this recommendation is followed, no data processing will take place by any of the listed third-party sub-processors."

2.1.2.2. Google Group Sub-processors

2.1.2.2.1. Google Workspace for Education

KL has stated that sub-processors for Google Workspace for Education are used for 'Data Centre operations', 'Service Maintenance' and 'TSS (Customer Initiated Support)'.

According to KL, the local authorities use the technical measure 'Data Regions' in connection with the processing of personal data in 'Data Centre Operations'. The 'Data Regions' measure means that the processing of personal data is restricted to a specific region. KL has stated that the local authorities only use services covered by 'Data Regions EU', which means that personal data is not processed outside the EU/EEA.

KL has further stated that not all services are covered by this measure. According to KL, there will therefore still be a limited amount of data that will be processed outside the EU/EEA. KL has stated that the processing of personal data in connection with 'Data Centre Operations' will consist of the storage of personal data.

Furthermore, KL has stated that sub-processors for Google Workspace for Education have limited access to 'Customer Data' in relation to 'Service Maintenance' and 'TSS'. KL has noted in this regard that 'Access Approvals' have been introduced for these processing operations, meaning that the sub-processor can only access 'Customer Data' if the customer grants them access.

KL has recommended that local authorities both use 'Access Approvals' and draw up procedures specifying when Google is to be granted access to personal data.

According to KL, there is a limited amount of personal data that is not covered by "Access Approvals". The local authorities cannot therefore ensure, through this measure, that personal data is not processed outside the EU/EEA.

KL has therefore stated that all sub-processors listed in KL's supplementary opinion of 23 June 2025 in the annexes entitled 'Annex 36: Kommunerelevante underdatabehandlere Google Workspace – OPDATERET JUNI 2025' and 'Annex 37: Kommunerelevante underdatabehandlere – Google Chrome', process data on behalf of the local authorities.

2.1.2.2.2. Chrome Education Upgrade

KL has stated that sub-processors for Chrome Education Upgrade are used for 'IT Facility Management', 'Service Support' and 'Technical Support Service/TSS'.

It also appears from KL's consultation response that KL has been in dialogue with Google regarding whether the technical measures in the form of "Data Regions" and "Access Approvals" can also be applied in connection with Google Chrome Education Upgrade. This is not the case, which is why all Google Groups sub-processors are relevant.

According to KL, it is therefore not possible for the local authorities to ensure that personal data is processed solely within the EU/EEA.

2.1.3. Locations

KL has provided lists specifying the locations of the sub-processors. The lists are set out in KL's supplementary opinion of 23 June 2025 in annexes entitled 'Annex 36: Sub-processors relevant to local authorities – Google Workspace – UPDATED JUNE 2025' and 'Annex 37: Sub-processors relevant to local authorities – Google Chrome'.

2.1.4. Lawfulness

KL has stated that personal data is transferred from the local authorities to Google Cloud EMEA, located in Ireland. Google Cloud EMEA then transfers personal data to Google LLC, located in the USA. The personal data will subsequently be transferred to Google Groups' sub-processors.

KL has stated:

"[…], that when the local authorities assess Google as a processor in accordance with Article

28(1), local authorities must also consider whether Google takes sufficient account of the level of data protection in the countries to which it transfers data when selecting sub-processors."

Furthermore, KL has stated that:

"The local authorities have entered into a data processing agreement with Google, which also regulates Google's use of sub-processors. It is stated, amongst other things, in the 'Cloud Data Processing Addendum' that Google enters into written contracts with all sub-processors and ensures that the sub-processor only has access to Customer Data to the extent necessary to fulfil the obligations under the contract. Google further states, as set out in Annex 35 to the case, that the same obligations to which Google is subject under the data processing agreement with the local authorities, in accordance with the Cloud Data Processing Addendum (Annex 9 to the case), will be transferred to the sub-processor."

and

"In addition, Google has confirmed that – as part of the selection process described in Annexes 11 and 12 – takes a number of aspects into account to ensure that the sub-processor has the necessary technical expertise and capacity and can provide the appropriate level of security and protection of personal data, including compliance with national data protection legislation."

It is KL's assessment "that the specified processors provide the necessary safeguards, and that the local authorities have verified this to a sufficient degree."

Furthermore, it is KL's assessment:

"[…], that the adequacy decision is in force, and that Google LLC is on the list of organisations registered under the Data Privacy Framework. KL has also established that the transfers fall within the scope of the adequacy decision."

2.1.5. List of disclosures to other independent controllers

KL has stated that any disclosures to other independent controllers take place only in accordance with the "Google Workspace for Education Terms of Service" and the "Chrome Enterprise Agreement".

3. Legal basis

According to Article 5(1)(a) of the General Data Protection Regulation, personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject. It further follows from Article 5(1)(f) of the Regulation that personal data must be processed in a manner that ensures appropriate security of the personal data in question, including protection against unauthorised or unlawful processing. In addition, pursuant to Article 5(2) of the General Data Protection Regulation, controllers are responsible for, and must be able to demonstrate, compliance with paragraph 1.

The processing of personal data is lawful only if one of the conditions set out in Article 6(1) of the General Data Protection Regulation is met. If the processing is based on Article 6(1)(c) or (e) of the Regulation, the legal basis for the processing must be provided for by Union law or the national law of the Member State to which the controller is subject, cf. Article 6(3).

Furthermore, Article 24(1) of the General Data Protection Regulation stipulates that the controller must implement appropriate technical and organisational measures to ensure and be able to demonstrate that the processing of personal data complies with the provisions of the General Data Protection Regulation. This must be done taking into account the nature, scope, context and purposes of the processing. The measures must be reviewed and updated where necessary.

Furthermore, Article 28(1)–(5) of the General Data Protection Regulation, concerning processors, stipulates the following:

1. Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.
2. The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.
3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:
(a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in

such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
(b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
(c) takes all measures required pursuant to Article 32;
(d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;
(e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;
(f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;
(g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;
(h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.
With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.
4. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.
5. Adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Article.
6. Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 3 and 4 of this Article may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 7 and 8 of this Article, including when they are part of a certification granted to the controller or processor pursuant to Articles 42 and 43.
7. The Commission may lay down standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the examination procedure referred to in Article 93(2).
8. A supervisory authority may adopt standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the consistency mechanism referred to in Article 63.
9. The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form.
10. Without prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.

With regard to point (h) of the first paragraph, the processor shall immediately inform the controller if, in its opinion, an instruction is contrary to this Regulation or to data protection provisions in other Union law or the national law of the Member States.

4. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member

State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.
5. Adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Article.

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

This decision has been taken on the basis of the annexes and the information which, since 23 June 2025 – following receipt of the local authorities' final statement and in light of the data processing agreement known as the Cloud Data Processing Addendum (dated 21 August 2025) (hereinafter the data processing agreement) – have formed part of the case.

4.1. Documentation of lawfulness

It follows from Article 5(2) of the General Data Protection Regulation that the controller is responsible for, and must be able to demonstrate, compliance with Article 5(1) of the General Data Protection Regulation concerning the principles governing the processing of personal data.

In line with this, Article 24(1) of the General Data Protection Regulation provides that:

"Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. [2]Those measures shall be reviewed and updated where necessary."

4.2. Substantive lawfulness of processing operations

4.2.1. Data processing agreement

According to Article 28(1) of the General Data Protection Regulation, the controller may only use processors who can provide the necessary guarantees that the processing of personal data will comply with data protection rules.

Furthermore, a processor's processing must be governed by a contract or other legal document under EU law or the national law of the Member States, which is binding on the processor in relation to the controller and which sets out the subject matter and duration of the processing, the nature and purposes of the processing, the type of personal data and the categories of data subjects, as well as the controller's obligations and rights, in accordance with the first sentence of Article 28(3) of the Regulation.

Google Cloud EMEA Limited (hereinafter 'Google') acts as a processor in connection with the local authorities' use of Google Workspace for Education and Google Chrome for Education.

The data processor arrangement is governed by the data processing agreement entered into between the local authorities and Google, and the use of sub-processors is governed by Section 11 of the data processing agreement.

Against this background, the Danish Data Protection Agency finds that the material submitted – taken as a whole – provides such a description of the processing scenario and the sub-processors used that the requirements listed in Article 28(3) can be verified and complied with.

This decision does not take a further position on the content of the data processing agreement. In this regard, reference is instead made to the Danish Data Protection Agency's previous decisions in this series of cases, including the cases with ref. no. 2020-431-0061.

4.2.2. Sub-processors

It follows from Article 28(4) of the General Data Protection Regulation that, where a sub-processor is used, the sub-processor must be subject to the same data protection obligations as those laid down between the controller and the processor.

The controller is not obliged to systematically request copies of sub-processor agreements in order to demonstrate that the processor's guarantees have been passed on to the sub-processor. However, the controller must be satisfied that the requirements have been passed on to the sub-processors, and this must be capable of being documented.

If the controller becomes aware that a (sub)processor is acting outside the original instructions, or if the processing arrangement otherwise gives cause for concern, the controller should request the relevant documentation and a copy of the agreement in that specific case.

In its Opinion 22/2024 on certain obligations arising from reliance on data processors and sub-processors, the EDPB has, amongst other things, stipulated that the controller must have a complete overview of which processors are processing personal data on the controller's behalf.

This means that the controller must have an overview of all processors and any sub-processors in the supply chain who process personal data on the controller's behalf.

According to the EDPB's opinion, this obligation entails that the controller must have the location and an authorised means of contacting all sub-processors, as well as a description of the processing activities and a clear delineation of the sub-processors' areas of responsibility. Furthermore, the controller must be able to produce this documentation at any time.

KL has stated that the local authorities' documentation is set out in KL's supplementary opinion of 23 June 2025 in annexes entitled "Annex 36: Local authority-relevant sub-processors – Google Workspace – UPDATED JUNE 2025' and 'Appendix 37: Sub-processors relevant to local authorities – Google Chrome', in which all of Google's relevant sub-processors are listed.

It is stated, amongst other things, in the data processing agreement between the local authorities and Google that:

"11.3 Requirements for Subprocessor Engagement. When engaging any Subprocessor, Google will:

a. ensure via written contract that:
i. the Subprocessor only access and uses Customer Data to the extent required to perform the obligations subcontracted to it, and does so in accordance with the applicable Agreement (including this Addendum); and
ii. if required under Applicable Privacy Laws, the data protection obligations described in this Addendum are imposed on the Subprocessor (as may be further described in Appendix 3 (Specific Privacy Laws)); and
b. remain fully liable for all obligations subcontracted to, and all acts and omissions of, the Subprocessor."

Against this background, the Danish Data Protection Agency considers that the requirements for Google are, at first sight, adequately reflected in the contracts with the sub-processors that Google chooses to use in connection with the processing of personal data on behalf of the local authorities.

The Danish Data Protection Agency attaches particular importance to the fact that, under the data processing agreement, if Google chooses to use sub-processors, the sub-processors are obliged to process data only to the extent necessary to fulfil the obligations arising from the contract. The sub-processors are also obliged to ensure that the processing of personal data takes place in accordance with the terms set out in the data processing agreement.

Furthermore, the Danish Data Protection Agency has emphasised that Google will be fully liable for all processing carried out by the sub-processors on behalf of the local authorities, in accordance with the principle set out in the last clause of Article 28(4) of the General Data Protection Regulation.

However, the Danish Data Protection Agency notes that the local authorities have not stated whether they have verified that the sub-processors are in fact complying with the requirements, or how the local authorities, as controllers, otherwise intend to verify this.

In this regard, it follows, inter alia, from the EDPB's opinion that:

"[…] the controller's obligation to verify whether the (sub-)processors present sufficient guarantees to implement the measures determined by the controller should apply regardless of the risk to the rights and freedoms of data subjects.

However, the extent of such verification will in practice vary depending on the nature of these organisational and technical measures determined by the controller based on, among other criteria, the risk associated with the processing."

Taking into account the information processed on behalf of the local authorities, and the risk that the processing poses to the rights and freedoms of data subjects, it is the Danish Data Protection Agency's assessment that the local authorities must specify in the documentation how and to what extent they will verify and monitor that the requirements are actually incorporated into the contracts with the sub-processors and that they are complied with by the sub-processors.

In this regard, the Danish Data Protection Agency assumes that the local authorities have the option of requesting a copy of Google's contracts with the sub-processors, at least insofar as they relate to the further processing delegated to the sub-processor.

The Danish Data Protection Agency further notes that the controller is obliged to request copies of contracts or other relevant documentation from processors and sub-processors if the controller becomes aware of any issues or otherwise deems it necessary.

4.2.3. Transfers to third countries

If the processing of personal data in question takes place, or is intended to take place under the contractual framework, through the engagement of a processor or sub-processor who processes personal data on behalf of the controller outside the EU/EEA, this will constitute a transfer of personal data to a third country.

Such a transfer will be covered by Chapter V of the General Data Protection Regulation on transfers of personal data to third countries or international organisations, under which a number of conditions apply to the processing of personal data.

Among other things, the controller must have a legal basis for the transfer in order to ensure its lawfulness. The assessment of which legal basis is most appropriate in a given situation varies depending on who the controller is, the country to which personal data is to be transferred, how quickly the legal basis must be established, and so on.

The controller must therefore, first and foremost, identify the countries to which personal data is transferred.

4.2.3.1. Locations

The Danish Data Protection Agency assumes that personal data is transferred from the processor Google Cloud EMEA Limited in Ireland to the sub-processor Google LLC in the USA. From there, personal data is further transferred to the other sub-processors specified.

The Danish Data Protection Agency assumes – in accordance with the information provided by KL in its statement of 23 June 2025 and the annexes entitled "Annex 36: Sub-processors relevant to local authorities – Google Workspace – UPDATED JUNE 2025' and 'Annex 37: Sub-processors relevant to local authorities: Google Chrome' – that the sub-processors listed process personal data on behalf of the local authorities in accordance with the agreement.

Against this background, the Danish Data Protection Agency notes that the sub-processors process personal data both within the EU/EEA, in safe third countries and in several unsafe third countries, including India, Mexico and Taiwan.

4.2.3.2. Basis for transfer in relation to the USA

Under Article 45(1) of the General Data Protection Regulation, the transfer of personal data to a third country or an international organisation may take place if the European Commission has determined that the third country, a territory or one or more specific sectors within that third country, or the international organisation in question, ensures an adequate level of protection.

If a cloud service provider carries out transfers on the basis of an adequacy decision, it is the Danish Data Protection Agency's view that the controller must still be able to demonstrate that 1) the adequacy decision is in force, and that 2) the transfer falls within the scope of the adequacy decision.

The European Commission has adopted an adequacy decision on the so-called EU-US Data Privacy Framework (DPF). However, the adequacy decision may only be used as a basis for transfers when personal data is transferred to organisations that have been certified under the DPF by the US Department of Commerce.

KL has stated that personal data from Google is transferred to Google LLC on the basis of the DPF. Furthermore, KL has stated that Google LLC is certified under the DPF and that the transfers fall within the scope of the adequacy decision.

On this basis, the Danish Data Protection Agency finds that the local authorities have established a sufficient legal basis for the transfer of personal data from Google to Google LLC by using the DPF.

4.1.2.3. Legal basis for onward transfers to sub-processors

It is stated in the DPF that if a processor and/or a sub-processor in a safe third country transfers personal data on behalf of the controller, the controller is, as a general rule, not obliged to verify the lawfulness of the rules applicable in the third country or international organisation governing that processor's and/or sub-processor's onward transfers of personal data received within the framework of an adequacy decision. This situation will have been addressed in the adequacy assessment.[2]

Furthermore, the DPF states that the level of protection for personal data transferred from the Union to organisations in the US must not be undermined by onward transfers of such data to a recipient in the US or another third country.[3] Onward transfers may only take place (i) for limited and specific purposes, (ii) on the basis of an agreement between the organisation under the EU-US Data Protection Framework and the third party in question (or a corresponding arrangement within a group of companies); and (iii) only if this agreement ensures that the

third party guarantees the same level of protection as the principles set out in the General Data Protection Regulation.

The Danish Data Protection Agency considers that onward transfers to sub-processors may therefore, as a general rule, take place on the basis of the DPF.

However, given that, as mentioned above, the DPF stipulates that the level of protection for personal data transferred from the Union to organisations in the US must not be undermined by the onward transfer of such data to a recipient in the US or another third country, the Danish Data Protection Agency considers it necessary to examine to which countries data is actually onward transferred and the adequacy of the level of protection in those third countries.

The Danish Data Protection Agency notes that, in this context, the European essential safeguards will form part of the assessment to be carried out to determine whether a third country provides a level of protection that is essentially equivalent to that guaranteed in the EU.[4]

The four essential European safeguards stem from the Schrems II judgment[5], paragraph 188, and are as follows:

"'effective administrative and judicial redress for the data subjects whose personal data are being transferred'". In this regard, Recital 104 of the General Data Protection Regulation emphasises that the third country 'should ensure effective independent data protection supervision authority and should provide for cooperation mechanisms with the Member States', and it is specified that "the data subjects should be provided and effective administrative and judicial redress."

To ensure an adequate level of protection, the local authorities must therefore ensure that these safeguards are reflected in the contracts that Google enters into with its sub-processors. Furthermore, it is essential to assess whether a contractual basis alone will provide a level of protection that is essentially equivalent to that in the EU/EEA.

KL has stated that Google's contracts with sub-processors impose on them the same obligations as those to which Google is subject under the data processing agreement with the local authorities. Furthermore, KL has stated that the safeguards provided under the DPF are carried forward into the contracts with the sub-processors.

However, in the Danish Data Protection Agency's view, this finding will not necessarily, in itself, be sufficient to ensure a level of protection for personal data that is essentially equivalent to that within the EU/EEA if (onward) transfers take place to unsafe third countries.

The controller is obliged, prior to the transfer, to carry out an assessment of the conditions in the recipient country with a view to determining whether the chosen legal basis for the transfer can, in practice, ensure an adequate level of protection for the transferred data in accordance with the four essential European safeguards. This may be done following an assessment of the effectiveness of the chosen basis for the transfer, for example in the form of a transfer impact assessment (TIA).

The Danish Data Protection Agency notes that the local authorities have not, as a matter of course, carried out a further assessment of the onward transfers to sub-processors.

The Danish Data Protection Agency considers that the following countries in the sub-processor chain should have been subject to an investigation before the local authorities entered into the contract with Google:

- Australia
- Chile
- Canada, as it is not specified whether the sub-processor is covered by the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA)

- India
- Mexico
- Singapore
- Taiwan
- Brazil[6]
- Hong Kong
- Japan, as it is not specified whether the sub-processor is subject to the Japanese Act on the Protection of Personal Information (APPI)

The Danish Data Protection Agency points out that there are no formal requirements regarding how such an assessment should be carried out or how the documentation should be presented. However, it is important that the assessment determines whether the four essential safeguards are met and whether the mechanism used for the transfer effectively ensures that the rights of data subjects are protected in a manner equivalent to the legal framework in the EU/EEA.

Reports have been drawn up for several countries; for example, the assessments in report EDPS/2019/02-13[7] and the two reports numbered 022-0716[8]. The results of these analyses are not necessarily accurate today, but they do provide an indication of the situation in the countries concerned. Although these analyses are more detailed than necessary in most processing scenarios, certain elements of them may nevertheless serve as inspiration for the considerations that a controller must undertake.

Furthermore, it follows from EDPB Opinion 22/2024 on certain obligations arising from reliance on processors and sub-processors that:

“Where personal data transferred by a (sub-)processor (on behalf of the controller) on the basis of an adequacy decision are subject to an onward transfer from this third country, the level of protection of natural persons guaranteed by the GDPR for such onward transfer should also not be undermined. In this regard, pursuant to Article 45(2)(a) GDPR, any adequacy decision issued by the European Commission covers, among others, the third countries’ rules governing onward transfers. Hence, under Article 44 GDPR, the controller does not have to check these requirements on its own.

In terms of the controller’s obligation under Article 28(1) GDPR, this means that the controller should ensure that the (sub-)processor provides ‘sufficient guarantees’ also with respect to onward transfers carried out by a (sub-)processor from an adequate country.”[9]

The controller is thus obliged to ensure – and be able to document – that a sub-processor complies with the relevant rules and has ensured that the level of protection is not undermined by the onward transfer.

In order to ensure this, it is necessary to note the following regarding the nature of adequacy assessments. These are based solely on the European Commission’s assessment of the conditions in the specific recipient country and may, furthermore, be limited to processing carried out by specific entities or in specific processing scenarios. For onward transfers outside the so-called ‘safe third country’ in question, this is enshrined in a contract between the (sub) processor in the safe third country and the sub-processor in the country to which the data is transferred.

Following the Schrems II judgment referred to above, the EDPB therefore published Recommendation 01/2020 on measures to supplement transfer mechanisms in order to ensure compliance with the EU level of protection of personal data.

Against this background, it is the Danish Data Protection Agency’s view that onward transfers of personal data to a country with what the EDPB, in the aforementioned recommendation, refers to as ‘problematic legislation’, cannot take place without supplementary measures, as long as such a onward transfer is based solely on a contract between the (sub-)processor in

the safe third country and the sub-processor in the unsafe third country. This is simply because the contract cannot definitively regulate the actions of public authorities in the unsafe third country.

The Danish Data Protection Agency notes that the local authorities have not documented whether this is the case.

The Danish Data Protection Agency acknowledges that, when entering into the contract, the local authorities examined the data processing agreement with Google and the requirements it imposes on sub-processors. The Danish Data Protection Agency is aware that Local Government Denmark (KL) has received confirmation from Google that a thorough screening is carried out of the sub-processors engaged by Google, and that the local authorities have the opportunity to monitor on an ongoing basis whether sub-processors are fulfilling their obligations. This can be done by reviewing reports which Google undertakes to make available.

However, the Danish Data Protection Agency cannot confirm that the reports on sub-processors have in fact been reviewed.

Against this background, and following an overall assessment of the processing activities described in the contract, in conjunction with the documentation submitted to the Danish Data Protection Agency, the Agency considers that the local authorities' 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) and Article 24, cf. Article 28(1) and (4).

Against this background, the Danish Data Protection Agency must, pursuant to Article 58(2)(b) of the General Data Protection Regulation, express **serious criticism** of the 51 local authorities.

In reaching this decision, the Danish Data Protection Agency has assumed that the 51 local authorities have configured their set-up of the programmes in question in accordance with the prerequisite and functional requirements specified by Local Government Denmark (KL), both in connection with the previous cases in this series of cases and as set out in relation to this case. These settings have been established, amongst other things, to exclude services involving processing for which there is no legal basis, particularly in relation to the disclosure of personal data to third parties.

Pursuant to Article 58(2)(a) of the General Data Protection Regulation, the Danish Data Protection Agency must warn the 51 local authorities that it is likely to be in breach of Article 6(1), cf. Article 6(3), unless they have configured the relevant programmes in accordance with the technical and functional requirements specified by KL, both in connection with the previous cases in this series of cases and as set out in this case.

Pursuant to Article 58(2)(a) of the General Data Protection Regulation, the Danish Data Protection Agency must also warn the 51 local authorities that it is likely to be in breach of Article 28(1) to engage a processor for the processing of personal data where such data is subject to further processing by a sub-processor in a third country where a level of protection essentially equivalent to that in the EU/EEA cannot be ensured.

It should be noted that, with regard to the Danish Data Protection Agency's exercise of its powers as a supervisory authority, particular weight has been given in this decision to the sanctions previously imposed for the various infringements identified, the clarification now provided by EDPB Opinion 22/2024, and the local authorities' general cooperation in clarifying the facts of the case.

5. Concluding remarks

The Danish Data Protection Agency notes that the entire course of events in this complex of cases could – and, in the Agency's view, should – have been avoided had the relevant data

protection assessments been carried out, evaluated and addressed before the specific product was procured, let alone put into use.

Furthermore, the Danish Data Protection Agency notes that it is neither possible nor lawful – under data protection law – to purchase and put into use a product that processes personal data if clarity cannot be established regarding the processing of personal data that takes place within the product. This applies regardless of the commercial rationale.

If a product is chosen where processing activities and the contractual basis on which the processing takes place change frequently, the controller must be able – on an ongoing basis – to document that the processing, even after the change, is carried out lawfully. If this is not possible, the processing must be discontinued or otherwise brought into compliance by changing the product and/or supplier.

This complex of issues, the number of data protection infringements and the work the local authorities – as a result – have had to carry out to ensure the lawfulness of their selection and use of the products in question, have led the Danish Data Protection Agency to urge organisations with similar processing scenarios to collaborate on drawing up common requirements during the procurement phase, common operational configurations during the operational phase and, in general, to consider making use of the option under Article 40 of the General Data Protection Regulation to draw up and have codes of conduct approved.

In future, the Danish Data Protection Agency will take this into account when determining sanctions if the principles set out in this decision and in previous decisions relating to this series of cases are not followed. This applies in particular to all areas where public authorities and institutional actors in the private sector carry out tasks in which users have limited choice of provider.

The Danish Data Protection Agency hereby considers the case closed and will take no further action in this matter.

[1] Opinion 22/2024 on certain obligations arising from reliance on processors and sub-processors

[2] See Article 45(2)(a) of the General Data Protection Regulation and the European Commission’s Implementing Decision (EU) 2023/1795 of 10 July 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on an adequate level of protection for personal data within the EU-US data protection framework, section 2.2.6.

[3] Ibid.

[4] In this regard, reference is made to EDPB Recommendation 02/2020 on the European essential safeguards for monitoring measures, page 5, paragraph 8

[5] CJEU Case C-311/2018 of 16 July 2020

[6] It should be noted that, following the adoption of the European Commission’s adequacy decision on 26 January 2026, Brazil is now considered to be a safe third country. However, at the time the local authorities entered into the contract with Google, Brazil was an unsafe third country.

[7] legalstudy_on_government_access_0.pdf

[8] study_on_government_access_to_data_in_third_countries_17042023_mexico_and_turkiye_final_report_milieu_redacted.pdf and study_on_government_access_to_data_in_third_countries_17042023_brazil_final_report_milieu_redacted.pdf

[9] EDPB Opinion 22/2024 on certain obligations arising from reliance on processors and sub-processors, paragraphs 94 and 95