DATATILSYNET

30 January 2024

The Danish Data Protection Agency issues an order in the Chromebook case

In the case concerning the use of Google Workspace in Danish primary and lower secondary schools, the Danish Data Protection Agency has concluded that there is no legal basis for the disclosure of personal data to Google for all the purposes for which it is currently being disclosed. The Agency has therefore issued an order to local authorities to bring their processing practices into line with the regulations and has outlined various ways in which this can be achieved.

Summary

Since the summer, the Danish Data Protection Agency has been reviewing the extensive material submitted by Local Government Denmark (KL) on behalf of 53 local authorities in the case concerning the use of Google Workspace in schools, and has, on that basis, reached a decision which is being published today.

The material has now provided a detailed description of the key aspects of the schools' use of the service and the provider's use of data. This was an original prerequisite for the local authorities to be able to start processing the information in Google Workspace, and the relevant analyses should therefore have been in place before the tools were put into use. This lack of clarification and the incomplete analyses have been assessed and sanctioned in the Danish Data Protection Agency's previous decisions against the 53 local authorities.

In the material now submitted, the local authorities acknowledge that there is a disclosure of personal data, which Google uses for its own purposes. The Danish Data Protection Agency has therefore assessed the lawfulness of these disclosures of personal data and reached a decision on this part of the case, as clarification of this matter is a prerequisite for processing the data at all. At the same time, this clarification sets out the framework for a solution whereby personal data relating to schoolchildren can be processed in future.

"Before putting a tool into use, a controller must gain an overview of how personal data is processed within it and must be able to document this. This requirement applies to all organisations. However, when it comes to public authorities – where we as citizens cannot opt out of having our data processed – the Danish Data Protection Agency has a particular expectation that the necessary analyses are both carried out and documented," says Allan Frank, IT security specialist and lawyer at the Danish Data Protection Agency, and continues:

"Most off-the-shelf IT products today have a highly complex contractual framework, which not only allows for many variations in the processing of personal data but also changes relatively frequently. This makes it more difficult than necessary for data controllers – whether businesses or public authorities – to comply with the GDPR, as it is easy to lose track of what is happening to the data. We at the Danish Data Protection Agency therefore urge that contracts

be made more transparent – not only in terms of the processing structure, but also in terms of the consequences when circumstances relating to the service provision change."

Order to legalise the disclosure

The conclusion of the Danish Data Protection Agency's decision is that there is a legal basis for disclosing pupils' information for the purposes of providing the services, improving the security and reliability of the services, communicating with, amongst others, the local authorities, and complying with legal obligations.

However, it is also assessed that the Danish Primary and Lower Secondary School Act does not provide a sufficiently clear legal basis for local authorities to disclose pupils' data for the maintenance and improvement of the Google Workspace for Education service, Chrome OS and the Chrome browser, or for measuring performance and developing new features and services in Chrome OS and the Chrome browser.

The Danish Data Protection Agency is therefore issuing an order to the local authorities to bring the processing into compliance with the rules by ensuring that there is a legal basis for all processing carried out. This can be achieved, for example, by:

The local authorities no longer passing on personal data to Google for these purposes. This will likely require Google to develop a technical solution to cut off the relevant data flows.
Google itself refraining from processing the data for these purposes.
The Danish Parliament providing a sufficiently clear legal basis for the disclosure of personal data for these purposes.

Local authorities must comply with the order from 1 August 2024, but must indicate by 1 March at the latest how they intend to comply with it.

"IT services today often operate in such a way that the disclosure of personal data is built into the product, and that the use of the data is often a prerequisite for deriving the full benefit from the products' functionality. However, this does not always take place with sufficient focus on the protection of the citizens whose data is being used. But neither the functionality of the solutions one wishes to use, the supplier's market position, the standardised structure, nor the mere use of a standard product can justify failing to comply with the data protection rules that politicians have decided we must have in Europe," says Allan Frank.

Which parts of the decision are still pending?

Based on the local authorities' feedback on 1 March 2024, the Danish Data Protection Agency will inform the local authorities of any further specific matters which – in addition to the changes that have already taken place and are described in the material submitted – must be addressed by the deadline for compliance on 1 August 2024. This partial decision depends on how the local authorities intend to comply with the order regarding the legal basis for the aforementioned disclosures, and is therefore a step-by-step process.

Decision

The Danish Data Protection Agency hereby returns to the case in which, on 14 July 2022, the Agency issued a prohibition to Helsingør Municipality against processing personal data using Google Chromebooks and Workspace for Education. The Danish Data Protection Agency upheld this prohibition by decision of 18 August 2022.

Following a subsequent dialogue with Helsingør Municipality, during which the municipality identified a number of instances where the use of Google Chromebooks and Workspace for Education had either not been lawful or where the risks to data subjects had not been sufficiently identified and mitigated, the Danish Data Protection Agency suspended the

aforementioned ban by a decision of 8 September 2022. At the same time, the Danish Data Protection Agency issued four orders to Helsingør Municipality.

Subsequently, in the period up to 24 October 2022, the Danish Data Protection Agency also issued the same four orders to the following 52 other local authorities:

1	Albertslund Municipality	19	Horsens Municipality	37	Slagelse Municipality
2	Allerød Municipality	20	Hvidovre Municipality	38	Solrød Municipality
3	Ballerup Municipality	21	Hørsholm Municipality	39	Sorø Municipality
4	Dragør Municipality	22	Ishøj Municipality	40	Svendborg Municipality
5	Egedal Municipality	23	Jammerbugt Municipality	41	Syddjurs Municipality
6	Fanø Municipality	24	Langeland Municipality	42	Thisted Municipality
7	Favrskov Municipality	25	Læsø Municipality	43	Tønder Municipality
8	Faxe Municipality	26	Mariagerfjord Municipality	44	Tårnby Municipality
9	Fredericia Municipality	27	Middelfart Municipality	45	Vejen Municipality
10	Faaborg-Midtfyn Municipality	28	Nordfyn Municipality	46	Vejle Municipality
11	Glostrup Municipality	29	Næstved Municipality	47	Vesthimmerland Municipality
12	Greve Municipality	30	Odder Municipality	48	Vordingborg Municipality
13	Gribskov Municipality	31	Odense Municipality	49	Ærø Municipality
14	Haderslev Municipality	32	Odsherred Municipality	50	Aalborg Municipality
15	Hedensted Municipality	33	Randers Municipality	51	Aarhus Municipality
16	Herlev Municipality	34	Rebild Municipality	52	Brøndby Municipality
17	Hjørring Municipality	35	Samsø Municipality		
18	Holbæk Municipality	36	Silkeborg Municipality		

KL subsequently informed the Danish Data Protection Agency on 12 September 2023 that KL and KOMBIT represent Helsingør and the 52 other municipalities mentioned above in the further processing of the cases by the Agency.

1. Decision

Having reviewed the material most recently submitted by KL on behalf of the 53 municipalities on 30 June 2023, the Danish Data Protection Agency – given the scope and complexity of the case – finds grounds to, as a first step, make a decision regarding the municipalities' disclosure of personal data to Google Ltd.

In this connection, the Danish Data Protection Agency finds that there are no grounds for disregarding the local authorities' assessment that, as part of their selection of teaching and learning resources for primary and lower secondary schools, it is necessary to process and transfer personal data to Google in connection with the use of Google Chromebooks and Workspace for Education for the purposes of (i) the provision of and (ii) improving the security and reliability of the services in question, etc. ("the original purposes"), cf. Article 6(1)(e) of the General Data Protection Regulation, cf. Article 6(3), and sections 2(1) and 18(1) of the Primary and Lower Secondary Education Act. This includes, amongst other things, the processing of personal data for the purpose of providing the services, improving the security and reliability of the services, communicating with, amongst others, the local authorities, and complying with legal obligations.

However, it is the Danish Data Protection Agency's assessment that the local authorities cannot, within the framework of sections 2(1) and 18(1) of the Danish Primary and Lower Secondary Education Act, cf. Article 6(1)(e) of the General Data Protection Regulation, process and disclose personal data relating to school pupils to Google as part of the use of Google Chromebooks and Workspace for Education for the purposes of (i) maintaining and improving the Google Workspace for Education service, Chrome OS and the Chrome browser, (ii) measuring the performance of Chrome OS and the Chrome browser, and (iii) developing new features and services in Chrome OS and the Chrome browser ('the secondary purposes').

Against this background, the Danish Data Protection Agency finds that there are grounds for issuing an order to the local authorities to bring their processing of personal data – in the form of the disclosure of personal data to Google – into compliance with Article 5(1)(a) and Article 6(1) of the General Data Protection Regulation, and to be able to demonstrate this, see Article 5(2) of the Regulation.

This may be achieved, for example, by:

the local authorities ceasing to transfer personal data to Google for the purposes in question, which is likely to require Google to develop a technical solution to cut off the relevant data flows, Google refraining from processing data for these purposes, or the Danish Parliament providing a sufficiently clear legal basis for the processing in question.

The Danish Data Protection Agency initially requests that the local authorities state how they intend to comply with the above order. The Danish Data Protection Agency requests that this statement be submitted by 1 March 2024 at the latest.

The deadline for compliance with the order is 1 August 2024. The Danish Data Protection Agency requests that confirmation of compliance with the order be provided by that date at the latest. The order is issued pursuant to Article 58(2)(d) of the General Data Protection Regulation.

Under Section 41(2)(4) of the Data Protection Act, a person who fails to comply with an order issued by the Danish Data Protection Agency pursuant to Article 58(2)(d) of the General Data Protection Regulation is liable to a fine or imprisonment for up to six months.

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

2. Statement of the case

Between 8 September and 24 October 2022, the Danish Data Protection Agency issued the following orders to 53 local authorities concerning their use of Google Chromebooks and Workspace for Education:

"The Danish Data Protection Agency hereby issues […] Municipality with an order to amend the agreement with the processor in such a way that the matters referred to in the Agency's decisions of 14 July and 18 August 2022, in relation to Helsingør Municipality, as well as the material […] the Municipality submitted on […] 2022, and which stems from the overall contractual framework with the ' ' provider, are brought into compliance with the General Data Protection Regulation. This includes, as a minimum, a clarification of the instances in which the 'processor' acts as an independent controller, as well as the purposes for which it does so; the support situations which the municipality no longer utilises; and ambiguities in [the contract text] that create uncertainty regarding the processor's actions beyond the provisions of Article 28(3)(a) of the General Data Protection Regulation. Furthermore, all intended transfers to non-safe third countries must demonstrably comply with the General Data Protection Regulation.

The Danish Data Protection Agency further issues […] Municipality with an order to describe the data flows taking place and to identify the personal data disclosed to the supplier, and to clarify when the latter acts as an independent or joint controller. The documentation must cover the entire technology stack that […] Municipality uses for the processing.

The Danish Data Protection Agency further orders […] Municipality to draw up an updated impact assessment based on all the risks identified by the municipality during the documentation process, should it transpire that – in addition to those for which an Article 36 procedure has now been requested – there are further high, non-mitigable risks, the order also includes consultation with the Danish Data Protection Agency pursuant to Article 36.

Finally, the Danish Data Protection Agency orders […] Municipality to submit a final, time-bound plan for bringing any processing operations into compliance with the law that could not be brought into compliance by the deadline for the orders, which is set at 3 November 2022. The Danish Data Protection Agency expects to receive documentation of compliance with the orders by the specified date."

On 12 September 2023, KL informed the Danish Data Protection Agency that KL and KOMBIT represent the aforementioned local authorities in the further handling of the cases by the Agency and would therefore submit a joint response on behalf of all affected local authorities.

KL subsequently forwarded, on 3 November 2022, evidence of compliance with the Danish Data Protection Agency's orders to the 53 local authorities. KL forwarded supplementary material in this regard on 4 November 2022.

On 4 November 2022, the Danish Data Protection Agency informed KL and the affected local authorities that the Agency's prohibition of 18 August 2022 was suspended until the processing of the material received had been completed. In this connection, the Danish Data Protection Agency stated that it expected to complete its review by the end of 2022.

In the period that followed, KL became aware that, in its view, there was a need to elaborate on and amend parts of the material so that the local authorities could comply more fully with the Danish Data Protection Agency's order. KL therefore requested on 2 December 2022 that the Danish Data Protection Agency await this additional material.

The Danish Data Protection Agency acceded to KL's request and set a deadline of 23 January 2023 for the submission of this additional material.

KL submitted this additional material on 23 January 2023. Following a meeting between the Danish Data Protection Agency, KL, Aarhus Municipality and KOMBIT regarding the material, KL concluded that the material submitted needed to be elaborated upon. KL therefore requested on 23 March 2023 that the Danish Data Protection Agency await this further elaboration.

On 16 June 2023, prompted by a reminder from the Danish Data Protection Agency dated the same day, KL stated that it expected to submit the supplementary material by the end of June 2023.

On 30 June 2023, the Danish Data Protection Agency received a comprehensive response with 32 annexes from KL, which also stated that the collection of documents constituted the affected local authorities' evidence of compliance with the Danish Data Protection Agency's order.

KL's response of 30 June 2023, together with its annexes, constitutes, in conjunction with the above, a comprehensive account of the case. KL's response of 30 June 2023, together with Annexes 16 and 26 thereto, is attached as an annex to this decision.

3. General remarks

First and foremost, the Danish Data Protection Agency acknowledges the considerable work carried out by the local authorities, as controllers, to comply with the Danish Data Protection Agency's order. There is now a comprehensive description of what data is processed, by whom and in what capacity. The local authorities' work has also led to changes in the services they use and the contractual terms under which those services are provided.

However, the Danish Data Protection Agency emphasises that this work should have been carried out before Google Chromebooks and Workspace for Education were put into use. The local authorities' processing of personal data prior to this work therefore, as the Danish Data Protection Agency has previously ruled, contravened several provisions of the General Data Protection Regulation.

Where several data controllers use the same systems and carry out broadly similar processing of personal data, the Danish Data Protection Agency considers that there is significant synergy in conducting joint assessments of risk factors, any impact assessments and mitigating measures.

Furthermore, the Danish Data Protection Agency urges that associations and bodies representing categories of controllers draw up codes of conduct in accordance with Article 40 of the General Data Protection Regulation (GDPR) with a view to specifying the application of the GDPR.

A code of conduct can provide accurate and practical guidance on how, in connection

one or more processing activities to comply with data protection rules. This may, for example, involve establishing procedures to be followed for a specific processing activity. A code of conduct will therefore be a useful tool to help the authorities that have adhered to the code comply with data protection rules.

Whilst adherence to and compliance with a code of conduct makes it easier to comply with data protection rules, it does not exempt individual local authorities from the duties and responsibilities incumbent upon them as controllers. This is particularly important in situations where the controller chooses to deviate from the provisions of the common concepts and processing operations, for example by using a system for other purposes.

3.1. On the lawful processing of personal data

The principle of legality in public administration (the principle of legality) means that a public authority's decisions and administration in general must be based on law or another legal basis.

With regard to data protection rules, this principle means that public authorities – in addition to ensuring that the authorities' own performance of their tasks is carried out in accordance with data protection rules – must also ensure that the IT solutions which the authorities decide to use to support the performance of their tasks fall within the framework of data protection law.

Public authorities must therefore ensure, and take measures to ensure, that they do not design, develop, procure or implement solutions that do not comply with data protection rules. This can be achieved, amongst other things, by public authorities setting out relevant requirements in their procurement procedures and project models to ensure that solutions are procured or developed in accordance with data protection rules. In the Danish Data Protection Agency's view, the scope of these requirements may vary, taking into account the nature, scope and purpose of the processing activity that the solution is intended to support, as well as the risks to citizens that may be associated with the use of the solution. In any event, these requirements must consist of more than just a single requirement for the supplier that the solution must comply with data protection rules. The requirements may, for example, reflect the measures which the authority has assessed as necessary to take on the basis of its risk assessment or impact assessment in order to ensure the lawfulness of the solution.

Finally, the Danish Data Protection Agency notes that the functionality of the solutions to be used, or the market position of the supplier to be selected, cannot justify a failure to comply with data protection rules. A standardised structure of the solutions or the mere use of a standard product cannot, either, justify a failure to comply with data protection rules.

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

4.1. Mapping of data flows and allocation of roles between the local authorities and Google

4.1.1. Allocation of roles

A data protection impact assessment must, in accordance with Article 35(7) of the General Data Protection Regulation, include, at a minimum, a systematic description of the planned processing activities and the purposes of the processing.

A fundamental prerequisite for assessing and documenting compliance with data protection rules is having knowledge of, and being able to describe, what information is being processed, for what purpose(s) and in what capacity.

Following the Danish Data Protection Agency's order, KL, in collaboration with Google, has mapped out the respective roles of the local authorities and Google in the local authorities' use of Google Chromebooks and Workspace for Education, as well as what personal data is processed, by whom and for what purpose(s).

Overall, the local authorities are the controllers for the processing of personal data in connection with their use of Google Chromebooks and Workspace for Education. KL has also stated that Google's role across the technology stack is as follows:

Technology stack	Data controller		Processor	
	Service Data	Custo-mer Personal Data	Service Data	Customer Personal Data
Chrome OS	Yes	Yes	No	No
Chrome browser	Yes	Yes	No	No
Chrome EDU Upgrade	Yes	No	No	Yes
Workspace for Education (including Chrome Sync)	Yes	No	No	Yes

KL has thus stated that Google is the controller for any processing of personal data that takes place in connection with the use of Chrome OS and the Chrome browser, and that Google is not a processor for the local authorities in this context.

Furthermore, KL has stated that Google is the controller for the processing of Service Data in Chrome EDU Upgrade and Workspace for Education, and that Google's processing of Customer Data in these two products takes place as a processor on behalf of the local authorities.

A description of the processing activities for which Google is the controller is set out in Annex 26 to KL's response (attached). The overview also contains a detailed description of the specific information being processed and of the specific purposes of the processing.

The Danish Data Protection Agency understands that Customer Data generally comprises content data, e.g. documents handled in Workspace etc., whilst Service Data primarily comprises derived diagnostic data concerning, for example, school pupils' use of the products.

4.1.2. Legal basis

The local authorities' use of Chromebooks and Workspace for Education is governed by two agreements with Google. These are the Google Workspace for Education Terms of Service (dated 26 September 2023) and the Chrome Online Agreement (dated 7 April 2022).

The agreements cover the products Workspace for Education[1] and Chrome EDU Upgrade[2], as shown in the overview of the technology stack above.

The Google Workspace for Education Terms of Service also refer, amongst other things, to the Cloud Data Processing Addendum (dated 26 September 2023), which thus constitutes the data processing agreement in respect of the Workspace for Education product.

Furthermore, the Chrome Online Agreement refers, amongst other things, to the Data Processing Amendment to Chrome Agreements (dated 16 February 2023), which constitutes the data processing agreement for the Chrome EDU Upgrade product.

In both sets of agreements, 'Customer Data' and 'Customer Personal Data' have specific meanings.

Service Data processed as part of the use of Workspace for Education and Chrome EDU Upgrade is defined in more detail in the Google Cloud Privacy Notice (dated 21 August 2023)

and is not covered by the local authorities' agreement with Google, but is processed by Google as the controller.

The local authorities' use of Chrome OS and the Chrome browser, as detailed below, is likewise not governed by agreements between the local authorities and Google.

Instead, according to Google, the use of Chrome OS is governed by Google's general Terms of Service[3] and Privacy Policy[4]. The Terms of Service are not entered into with the local authorities, but with the individual end-users, who in this case are school pupils (and their parents).

Similarly, the following is stated at the bottom of page 3 of Annex 26:

"Today, Google acts as a data controller when providing ChromeOS and Chrome browser, for both Customer Data and Service Data. As part of providing Chrome services, Google processes personal identifiers relating to devices or end users of Chrome, which are only used for the purposes set forth in the Google Privacy Policy."

Against this background – and in light of the division of roles between the local authorities and Google, as outlined by KL – the Danish Data Protection Agency considers that the use of the Chrome browser is not governed by an agreement between the local authorities and Google, but is instead governed by Google's general terms of service and privacy policy, as is also the case for Chrome OS.

4.1.3. The purposes of the processing of personal data

In its dialogue with Google, KL has found it necessary to clarify the contractual basis with Google regarding the purposes for which Google processes the data. As part of its response of 30 June 2023, KL has submitted a draft contract amendment which specifies, amongst other things, the purposes for which Google may process the data.

For Workspace for Education, Google will henceforth process Customer Data as a processor on behalf of the local authorities to provide the service and support (upon request from the local authorities). Google has also clarified that Customer Data will not be processed for marketing purposes or to improve Google's products and services, including Workspace for Education.

Google has further undertaken, as controller, to process only Service Data generated through the use of Workspace for Education in order to improve and optimise the performance, reliability, core functionality, availability, data protection, security and efficiency of the IT infrastructure of (a) Google Workspace for Education and related support, and (b) Google Cloud, Google Cloud Marketplace and Google Workspace Marketplace services, provided that the local authorities use such services. Google will not process Service Data to improve or optimise other Google products or services.

For Chrome EDU Upgrade, Google will process Customer Personal Data to:

(a) to provide, secure and monitor the Services and any TSS requested by the Customer; (b) to support the Customer's and its End Users' secure and compliant use of the Services; (c) as described in this Data Processing Amendment, including Sections 10 (Data Transfers) and 11 (Subprocessors); (d) as described in Section 7 (Confidentiality; Legal Process) of the Agreement, provided that any disclosure by Google or any Sub-processor with its address in the EEA complies with European data protection law; and (e) as further specified via (i) the Customer's compliant use of the Services (including the Admin Console and other Services functionality) and any TSS requested by the Customer, and (ii) any other written instructions given by the Customer and acknowledged by Google as constituting instructions under this Addendum"

KL has further stated that Service Data processed as part of the Chrome EDU Upgrade is a subset of the Service Data processed as part of the Chrome browser.

Furthermore, KL has stated that Google is the controller for the processing of all personal data, regardless of whether the data is characterised as Service Data or Customer Personal Data, in connection with the use of Chrome OS and the Chrome browser.

The purposes of Google's processing of Service Data in Chrome EDU Upgrade, and of all other personal data in Chrome OS and the Chrome browser, are set out in Google's privacy policy[5].

In summary, KL has stated that Google processes personal data, for which the company is the independent controller, across the technology stack for the following purposes:

Service	Original purposes	Derived purposes
Workspace for Education	To provide the cloud services requested by local authorities To provide recommendations on optimising the use of cloud services Assist local authorities Protect local authorities, Google's users, customers, the public and Google Comply with legal obligations	Maintain and improve cloud services Provide and improve other services requested by local authorities
Chrome OS	Provide Google's services Improve the security and reliability of services Communicate with customers Provide personalised services (Google Sync)[6] Comply with legal obligations	Maintain and improve Google's services Measuring performance Develop new features and services
The Chrome browser	Deliver Google's services Improve the security and reliability of services Communicate with customers Provide personalised services (Google Sync)[7] Comply with legal obligations	Maintain and improve Google's services Measuring performance Developing new features and services

Finally, KL has provided a more detailed description of the above-mentioned purposes and how personal data is processed in connection with these purposes. This is set out in Annex 26 to KL's response (attached).

4.1.4. The Danish Data Protection Agency's assessment

Following a review of KL's response, the Danish Data Protection Agency finds that the local authorities have described which personal data is processed in connection with their use of Chromebooks Workspace for Education, as well as the roles of the local authorities and Google in the processing of personal data. The description covers the entire technology stack.

The Danish Data Protection Agency therefore considers its order to describe the data flows taking place and to specify which personal data is disclosed to Google to have been complied with.

However, the Danish Data Protection Agency notes that the description of the data flows and the contractual framework governing the local authorities' use of Chromebooks and Workspace for Education is complex. In the Agency's view, this in itself entails a risk of non-compliance with data protection rules. This is because even minor changes to the technology stack or the contractual framework may entail changes in consequences that the local authorities may overlook.

The Danish Data Protection Agency therefore urges local authorities to engage in further dialogue with Google with a view to simplifying, in particular, the contractual framework, or to ensure that they possess or have access to the necessary technical and legal expertise to ensure compliance with data protection rules.

4.2. Disclosure of personal data

4.2.1. The General Data Protection Regulation

Personal data may be processed on the basis of one of several legal grounds set out in Article 6(1) of the General Data Protection Regulation. For public authorities, the processing of personal data will most often take place because it is necessary to comply with a legal obligation, see Article 6(1)(c), or because the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, see Article 6(1)(e).

In both cases, the processing must have a so-called supplementary legal basis, which obliges or entitles the authority to carry out a specific official task. This follows from Article 6(3) of the General Data Protection Regulation.

4.2.2. Requirements for the supplementary legal basis

Article 6(3) of the General Data Protection Regulation sets out several requirements for the supplementary legal basis, which must therefore meet certain criteria.

Firstly, Article 6(3), first sentence, requires that the basis for the processing must be provided for by EU law or national law.

Recital 45 of the preamble states that the General Data Protection Regulation does not imply that a specific law is required for each individual processing operation under Article 6(1)(e). A single law may suffice as the basis for several data processing activities. However, there is a requirement that processing under that provision must be based on EU law or national law. Furthermore, it follows from Recital 41 of the General Data Protection Regulation that the legal basis in question does not necessarily require a law, but that the legal basis should nevertheless be clear and precise, and its scope should be predictable for data subjects falling within its scope.

The Ministry of Justice's Report No. 1565/2017, pp. 132 et seq., states the following regarding Article 6(1)(e) of the Regulation:

"In this context, it must be assumed that Article 6(1)(e) is directly applicable as a basis for processing, provided that the controller is carrying out a task in the public interest or in the

exercise of official authority vested in the controller. The use of Article 6(1)(e) as a basis for processing does not, therefore, require national implementing legislation governing the actual processing of personal data in connection with the performance of tasks carried out in the public interest or in the exercise of official authority.

Nor does the use of Article 6(1)(e) necessarily require that the task requiring the processing of personal data be expressly imposed on the authority by legislation. In this connection, reference may be made to [the Danish Data Protection Agency's opinion in case no. 2004-54-1394], in which the Authority considered it natural that the Ministry of Education, as the central authority in this area, should carry out a task relating to digital registration for and applications for admission to educational programmes, even though there was no explicit statutory basis requiring the Ministry to perform that task. The Ministry could therefore rely, inter alia, on Section 6(1)(5) of the Data Protection Act concerning processing necessary for the performance of a task carried out in the public interest."

Furthermore, the following is stated on page 160 of the report regarding Article 6(3) of the Regulation:

"It also follows from the second sentence of Article 6(3) of the Regulation, specifically concerning processing referred to in Article 6(1)(e) – that is, for the purposes of performing a task carried out in the public interest or in the exercise of official authority – that the processing must be 'necessary for the performance of a task carried out in the public interest or in the exercise of official authority'. Here too, it must be sufficient to satisfy this requirement of necessity that this can be inferred from the relevant national legislation and its preparatory works, provided that the processing is in fact 'necessary'.

The final clause of Article 6(3) sets out a further requirement for the legislation transposing the General Data Protection Regulation. It requires that Member States' national law must serve a purpose in the public interest and be proportionate to the legitimate aim pursued. The General Data Protection Regulation thus lays down a requirement for proportionality and the observ of the public interest in relation to national and EU law that adapts the application of the General Data Protection Regulation."

In connection with the Ministry of Justice's national evaluation of the data protection rules in April 2021, the Danish Data Protection Agency stated, amongst other things, the following in a submission to the Ministry:

"The provisions of Article 6(2) and (3) of the Regulation imply, firstly, that processing – in order to be carried out pursuant to Article 6(1)(e) – must be provided for by EU law or the national law of the Member States. This means that the application of Article 6(1)(e) requires that the processing be provided for in EU law or national law, but not necessarily that there be national implementing legislation specifically authorising the processing itself. […]

In other cases, however – and in the vast majority of cases – the specific legislation will not contain specific requirements regarding the processing of personal data or otherwise stipulate specifically whether, and which, personal data are to be processed. The processing of personal data will, however, typically be a prerequisite for the authority to carry out the tasks prescribed by law. This could, for example, involve a public authority's assessment of a citizen's entitlement to social benefits under social legislation or legislation governing the authority's duties in the areas of children and education.

In such cases, determining when processing under Article 6(1)(e) of the Regulation may be considered necessary must be assessed in the light of the tasks and obligations incumbent on the authority under the legislation governing its activities. The same applies in relation to the requirement of necessity set out in Article 5(1)(c) of the Regulation.

In this context, it is important to emphasise that the data protection rules are not intended to hinder or complicate the performance of public authorities' tasks. The data protection rules,

including the requirement of necessity, do not therefore imply that public authorities must, at all costs, organise the performance of their tasks in such a way as to process as little personal data as possible, if this would prevent the authority from carrying out its tasks in the manner intended by the legislation.

The data protection requirement of necessity is, on the other hand, flexible and allows the controller – in this context, public authorities – to assess what is, in each individual case, relevant and objective, i.e. necessary, for the authority to carry out its tasks in the manner intended by the legislation. In this connection, it is also important to bear in mind that the authority which is required by law to carry out a task is, by its very nature, best placed to assess what is objective and relevant to the performance of that task, as it is precisely that authority which has the greatest knowledge of how any sector-specific legislation is implemented in practice.

It will therefore fall within the scope of Article 6(1)(e) of the General Data Protection Regulation if the authority can cite a legal basis as the reason for the processing, and if the processing is not – from a general perspective – unduly intrusive for the data subject, for example, because the processing is merely a practical means for the authority to fulfil its purpose, which does not take the data subjects into account.

In other words, public authorities have a fairly broad scope for assessing which processing of data is necessary to carry out the authority's tasks in accordance with the law."

Finally, the Court of Justice of the European Union states the following in its judgment of 24 February 2022 in Case C-175/20[8]:

"In that context, it should nevertheless be recalled that, in order to satisfy the requirement of proportionality to which Article 5(1)(c) […] gives expression […], the legislation which provides the basis for the processing must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose personal data are affected have sufficient guarantees that those data will be effectively protected against the risk of abuse. That legislation must be legally binding under domestic law and, in particular, must indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary."

The requirement for clarity in the relevant legal basis therefore generally depends on how intrusive the processing of personal data carried out by the solution will be for the citizen. If the processing is entirely harmless, the requirements will be less stringent than in the case of intrusive processing, where greater clarity is required in the legal basis.

4.2.3. The Primary and Lower Secondary Education Act

The local authorities' regulatory responsibilities in the school sector are set out in the Primary and Lower Secondary Education Act[9]. Sections 1(1) and 2(1) of the Act state the following:

"Section 1. In cooperation with parents, the primary school shall provide pupils with knowledge and skills that: prepare them for further education and inspire them to learn more; familiarise them with Danish culture and history; give them an understanding of other countries and cultures; contribute to their understanding of humanity's interaction with nature; and promote the all-round development of each individual pupil. […]

"Section 2. The local authority is responsible for the primary and lower secondary school, subject, however, to Section 20(3), Section 44 and Section 45(2), second sentence. The local authority is responsible for ensuring that all children in the municipality are guaranteed the right to free education in the primary and lower secondary school."

Furthermore, the following arises from Section 5(1) and (2) of the Act:

“Section 5. The content of teaching shall be selected and organised in such a way as to enable pupils to gain in-depth knowledge of subjects, an overview and an understanding of interrelationships. Teaching must enable pupils to acquire the methods of inquiry and working practices specific to each subject. In conjunction with this, pupils must have the opportunity to apply and develop the knowledge and skills they have acquired through teaching on cross-curricular themes and issues.

Subsection 2. Teaching in Years 1–9 is organised into three subject blocks and comprises, for all pupils: […]”

The preparatory work for the provision (Folketingstidende 1992–93, Supplement A, Bill of 22 April 1993, col. 8939) states the following:

“For all subjects in the three groups, it is important to note that IT must be integrated, as described in the teaching guidelines for the compulsory subject ‘IT’ under the current Act and in the supplements to the subject syllabuses issued by the Ministry in recent years. The integration of IT provides opportunities for the development of the subjects’ topics, concepts and methods, and examples of this will be included in future teaching guidelines.”

In this context, the following is stated in the preparatory work for Section 7 of the Act ibid., col. p. 8943), which sets out the compulsory subjects to be included in primary school education:

“It is proposed that IT be abolished as a compulsory subject, on the assumption that its content will be integrated into the compulsory subjects at the earliest year groups. In this way, all pupils will gain a basic understanding of the concepts and methods of information technology and an awareness of where computers can be usefully applied in the subjects. This knowledge is to form the basis for the general integration of IT into the subjects; see also the comments on Section 5 of the Bill.”

It is also evident from Section 18(1) of the Primary and Lower Secondary Education Act, which deals, amongst other things, with the choice of teaching materials:

“The organisation of teaching, including the choice of teaching and working methods, approaches, teaching materials and selection of subject matter, must in all subjects be consistent with the objectives of the primary and lower secondary school, the subject-specific aims and topics, and must be varied so as to meet the needs and abilities of the individual pupil.”

Furthermore, Section 19(1) of the Act states the following:

“The necessary teaching materials must be made available to pupils free of charge. However, this does not apply to instruments and equipment used in extracurricular teaching pursuant to Section 3(6) and which are taken home by pupils for their own use.”

The preparatory work for the provision (Folketingstidende 1992–93, Supplement A, Bill of 22 April 1993, col. 8956) states the following:

“As a result of information technology having evolved from being a compulsory subject to becoming an integral part of the content of other subjects, it is assumed that the ongoing development of equipping schools with information technology teaching resources and providing teachers with the necessary pedagogical background will continue, so that the aims of fully integrating IT can be realised within the next few years.”

The introduction of IT as a compulsory subject was affected by Act No. 435 of 13 June 1990. In support of the introduction of the subject as a compulsory subject, the Ministry of Education – as provided for in the preparatory work for the provision (Folketingstidende 1989–90,

Supplement A, Bill of 14 March 1990, p. 5194) – prepared a model curriculum and teaching guidelines. The curriculum and teaching guidelines state the following regarding the purpose of the IT subject:

“Aims of the compulsory module on IT

– pupils must become familiar with the use of hardware and software.

– pupils must gain an understanding of how computers are used in communication and problem-solving processes.

– pupils must gain an understanding of how the use of computers affects communication and problem-solving processes.

Comments on the purpose

Throughout history, people have communicated with one another using sounds, images, writing, etc. In many of these communication processes, they have used tools such as pencils, paintbrushes, typewriters and telephones. Such tools will always influence how people communicate with one another. The same applies when we solve problems.

The use of computers has become so widespread that it is fair to say that they are a tool which everyone will come to use. Many other tools are largely geared towards physical processes. This is not the case with computers, as this tool predominantly supports processes of an intellectual nature.

It is therefore of the utmost importance that people are able to incorporate IT appropriately into communication and problem-solving processes. At the same time, this will be an essential prerequisite for functioning effectively in a society where democratic decision-making processes and social norms are taken for granted. These are, therefore, prerequisites that all citizens must possess, and which must consequently form part of general education on a par with, for example, the ability to read, write and do arithmetic.

The purpose of IT education comprises three aspects:

– the operational aspect, which concerns general operational skills and an understanding of the overarching principles of how a computer works. The teaching must result in pupils becoming familiar with working on a computer and, through this, developing an appropriate understanding of how hardware and software work and interact. This is put into practice in the teaching programmes.

– the conceptual aspect, which concerns knowledge of the concepts and methods used when computers are employed for communication and problem-solving. The teaching should result in pupils becoming particularly aware of the common features – in the form of concepts and methods – found in virtually all computer applications. Such awareness will help to create structure in the pupils’ computer knowledge.

– the ‘significance’ aspect, which relates to an understanding of the role the computer plays in the process when it is used in connection with human communication or problem-solving. The teaching should ensure that, in their subsequent use of the computer, pupils are aware of whether the use of IT in these processes alters the conditions and outcomes.

It is important to emphasise that the main aim of the teaching is to ensure that pupils have options for action in practical situations. Pupils will only have such options for action if the use of IT is not dominated by technical problems or by their lack of knowledge of basic IT concepts and methods (see the section ‘Characterisation of IT teaching’). Teaching must therefore help pupils to become capable of using IT appropriately.

It should also be emphasised that it is important for pupils to realise that, through users' choice of different programmes, the computer can be used to solve many diverse tasks. This means that the computer is one of the most flexible tools at our disposal, and that we are often forced to decide whether, and if so how, we wish to use it. In many areas, starting to use computers will bring about major changes compared with the use of previous technology: it can open up entirely new possibilities, but it can also introduce new limitations compared with what was previously possible."

4.2.4. The Digitalisation Strategy 2011–2015

In its analysis and assessment, KL has on several occasions referred to the joint public sector digitalisation strategy for 2011 to 2015, which was drawn up in August 2011 by the government of the time, the local authorities and the regions.[10]

The use and development of digital learning resources was a key focus area in this strategy, which emphasises in several places that primary and lower secondary schools must keep pace with the times. KL has referred in this context to Annex 3.1.a to the strategy, which states, amongst other things:

"In connection with the financial injection, there is a need for a discussion with the digital learning resources sector on how they can be committed to working towards developments that support some of the visions described above. Among other things, discussions could focus on how to encourage private sector players to help translate and adapt tried-and-tested foreign digital learning resources to Danish conditions with a view to their sale."

KL has also referred to Annex 3.4 of the strategy, which states, amongst other things:

"A prerequisite for the success of the IT initiative is that IT is integrated into the development of new forms of teaching and learning, so that traditional teaching is not simply continued with 'power switched on'. There is therefore a need, through trials and research, to generally raise the level of knowledge regarding how to most effectively enhance pupils' academic and social learning using IT tools, including knowledge of how teachers can organise and support teaching using digital teaching materials and digitally-based learning programmes."

Finally, KL has referred to the agreement between the Government and KL on local authority finances for 2012. This states, amongst other things, the following:

"Enhanced use of IT in primary and lower secondary schools

Digital learning processes are already part of many Danish primary and lower secondary schools, but a more fundamental transformation is needed. It is therefore part of the joint public sector digitalisation strategy that, in the coming years, the focus will be on increased use of IT, so that it becomes an integral part of teaching in Danish primary and lower secondary schools.

IT should help to strengthen pupils' academic skills and better equip them for future educational and career opportunities, support a more targeted organisation of teaching, and enable better utilisation of resources in primary and lower secondary schools.

The Government and KL have therefore agreed on an ambitious initiative, under which the Government has earmarked

DKK 500 million from the Welfare Technology Fund over the coming years to:

Contribute to developing the market for digital learning resources, including stimulating a wide range of high-quality products.
Support effective distribution channels that ensure easy and straightforward access to digital learning resources, including providing access to digital learning objectives.

Help to disseminate lessons learnt from pilot and research projects, including providing limited support to demonstration schools, so that the development of IT-based forms of learning is focused on areas and subjects where the impact is greatest.

The Government and KL agree that the funds shall be allocated in accordance with the principles set out in Annex 2. Any contributions towards the purchase of teaching materials shall be co-financed by the local authorities, at a level at least equivalent to the central government's share.

To facilitate the transition in this area, the agreement stipulates that, by 2014 and within the current investment frameworks, the local authorities will ensure that all pupils have access to the necessary IT infrastructure, including stable and secure wireless networks with sufficient capacity, secure storage, power supply, etc."

4.2.5. The Danish Data Protection Agency's assessment

In the Danish Data Protection Agency's view, public authorities have, as provided for in the General Data Protection Regulation, its recitals, and the Ministry of Justice's Report No. 1565/2017, broad scope to process personal data where this is necessary for the performance of their official duties.

The Danish Data Protection Agency recognises that the aforementioned 'necessity requirement' is flexible and affords public authorities a broad margin of discretion to assess what, in each individual case, is relevant and objective – i.e. necessary – for the authority to carry out its tasks in the manner intended by the legislation.

The question then is to what extent local authorities can extend this flexibility to include the use of teaching and learning resources which, by virtue of their design and delivery model, entail the local authorities transferring personal data to another independent controller, the provider of the learning resources – in this case, Google – for the purposes of (i) delivering and (ii) improving the learning resources, as well as (iii) developing new features and services.

To begin with, the Danish Data Protection Agency notes that KL has stated that the assessment of whether the local authorities have a legal basis for disclosing personal data to Google must be carried out in two stages. Firstly, it is assessed whether the local authorities have a legal basis for disclosing personal data to Google for the purpose of providing the service. Secondly, it must be assessed whether the local authorities have ensured that Google may lawfully receive and process the personal data for other purposes, including the development of new features and services, in accordance with Article 5(1)(a) of the General Data Protection Regulation.

It is the Danish Data Protection Agency's view that the assessment of whether the local authorities have a legal basis for the disclosure of personal data to Google must be carried out in the light of all the purposes for which the data is to be processed. The local authorities must therefore assess whether there is a legal basis for the disclosure of personal data for the purpose of providing the service and for other purposes, including the development of new features and services. This includes all the purposes for which the local authorities are aware, at the time of disclosure, that the data will be processed.

The Danish Data Protection Agency refers in particular to its decision concerning Helsingør Municipality of 18 August 2022. This states, amongst other things, the following:

"The information may therefore not be lawfully 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."

It is the view of the Danish Data Protection Agency that the processing of personal data provided for in the provisions of the Primary and Lower Secondary Education Act concerning compulsory education, and which may therefore be carried out under Article 6(1)(e) of the General Data Protection Regulation, does not include the disclosure of such data to other independent controllers, including for purposes such as the further development of technology providers' applications, etc. It is the Danish Data Protection Agency's view that the disclosure of personal data by public authorities to private controllers generally requires a separate legal basis when the purposes in question fall outside the official duties that the public authority is required to perform."

The local authorities cannot, therefore, first assess whether there is a legal basis for the disclosure of personal data for certain purposes (the provision of the service) and then assume that the other purposes (development of new products, etc.), for which the personal data is also processed, must be regarded as Google's own further processing of the personal data for other purposes under Article 6(4) and (1) of the General Data Protection Regulation.

In this connection, the Danish Data Protection Agency attaches particular importance to the fact that the processing in question is specified in the contractual basis and is a prerequisite for the performance of the processing; the situation cannot therefore be equated with a scenario where, following a disclosure, a third party, acting as an independent controller, subsequently chooses to use personal data for its own new purposes.

KL has stated, in general terms, that the Primary and Lower Secondary Education Act stipulates that IT and digital learning resources must be fully integrated into teaching, and that the joint public sector digitalisation strategy for 2011 to 2015 focuses on working with the digital teaching resources sector to achieve greater integration of digital learning resources into teaching, including the development of new teaching and learning resources.

KL has further stated that, when using digital tools, it is necessary to utilise technical data to continuously develop and improve the tools. Over time, local authorities would end up with outdated products if suppliers did not continuously improve and develop the tools. The development of digital teaching resources has, as stipulated by the Primary and Lower Secondary School Act, the Joint Public Sector Digitalisation Strategy 2011–2015 for the primary and lower secondary school sector, and the financial agreement, taken place on an ongoing basis. In KL's view, teaching in primary and lower secondary schools will not meet the requirement in the Primary and Lower Secondary Education Act for the full integration of IT or digital teaching resources into the curriculum if these teaching resources are not continuously refined through development, updating and improvement.

Finally, KL has stated that the Joint Public Sector Digitalisation Strategy 2011–2015 states that 'the purpose of digital learning processes is to strengthen pupils' academic skills and better equip them for the future.'[11] In KL's view, it will not be possible to equip pupils for the future using yesterday's digital learning resources. In this context, it is not unexpected for local authorities that the products they procure should be improved and developed. It is also the wish of the local authorities that the products keep pace with the times.

As stated in the Danish Data Protection Agency's decision of 14 July 2022 concerning Helsingør Municipality, the local authorities, as part of their responsibility for the primary and lower secondary school system, have the right and duty to organise teaching so that it meets the objectives of the primary and lower secondary school system as well as the objectives for the individual subjects. This includes, amongst other things, the choice of teaching and working methods, teaching materials, etc. This follows from section 2(1) and section 18(1) of the Primary and Lower Secondary Education Act.

In the opinion of the Danish Data Protection Agency, these provisions also entail a certain scope for processing personal data where this is necessary as part of the local authorities' selection of teaching and learning resources.

The majority of the information that Google receives and processes for its own purposes as part of the local authorities' use of Google Chromebooks and Workspace for Education consists of metadata relating to individual pupils' use of the tools. This includes, amongst other things, information about the computer's settings, information about the use of the tools, applications, the Chrome browser, etc.

Google has informed KL that the purpose of processing this information can broadly be divided into (i) original purposes and (ii) secondary purposes. According to Google, the original purposes are inextricably linked to Google's provision of the tools and services in question to the local authorities. All the personal data in question is initially received and processed for this purpose. Furthermore, the secondary purposes enable Google to deliver value to customers and end-users in relation to their use of the tools and services in question and otherwise fulfil Google's obligations as the controller.

With regard to the secondary purposes, Google has stated that these include, amongst other things, (i) the maintenance and improvement of the Google Workspace for Education service, Chrome OS and the Chrome browser, (ii) measuring the performance of Chrome OS and the Chrome browser, and (iii) developing new features and services in Chrome OS and the Chrome browser.

Google has also explained how the company processes the data for these secondary purposes:

"When processing for these purposes, Google engineers do not use (and have no interest in using) personal data about specific end users or administrators at an individual level. Google has no interest in (for example) understanding whether and how a specific user uses a specific tool in one of its services, but Google does have an interest in understanding whether and how Google's users in general, on an overall level, use that tool. This means that Google's staff do not access or use any specific identifiers […] relating to any end user when processing for these purposes.

For example, in the context of ChromeOS, Google has no interest in processing an end user's specific device ID or serial number in order to "measure performance", but Google has an interest in processing large datasets of numbers of managed devices per country, regions, licenses, feature usage and failure rates etc keyed to a pseudonymous ID to understand the revenue distributions and generate insights of areas where Google needs to improve and – as such – "measure performance"."

The Danish Data Protection Agency assumes that, as part of their use of Chromebooks and Google Workspace for Education, the local authorities process and disclose personal data to Google, and that this data is processed solely for the original purposes and the secondary purposes as stated by KL.

Furthermore, the Danish Data Protection Agency assumes that, with regard to the secondary purposes, the data is processed solely for the development and improvement of services procured by the local authorities, and that Google does not process this data – or other data such as content data – for marketing purposes.

In light of the aforementioned amendments to the Primary and Lower Secondary Education Act, the Danish Data Protection Agency considers that it must be regarded as the intention of the legislature that IT should form an integral part of primary and lower secondary education. This was particularly evident with the introduction of IT as a compulsory subject, in which pupils were required to acquire knowledge of how IT could be used in communication and problem-solving processes, and how the use of IT affects such processes. Since then, the integration of IT has been expanded, as the compulsory subject was abolished and IT became an integral part of all subjects in primary and lower secondary schools.

The Danish Data Protection Agency also recognises that, over a number of years, there have been developments in how IT systems and services are delivered. Since the 1990s, there have been significant changes in architecture, functionality and delivery models. It is now far more common for suppliers of IT systems and services to collect and measure information on the use of the systems. This is done with a view to utilising the full functionality of the solutions and continuously improving the service provided, and is greatly facilitated by the widespread use of the internet and the increasing amount of computing power available.

However, the Danish Data Protection Agency notes that this development has not necessarily taken place with the necessary focus on data protection rules and consideration for the individual citizen. Although requirements for the lawful processing of personal data have been virtually identical in Denmark since the introduction of the Personal Data Act in 2000, controllers have not, to the extent necessary, imposed requirements on their suppliers of ITsystems and services to the extent necessary to ensure that developments in the way IT services are delivered took place within the framework of data protection rules.

Overall, the Danish Data Protection Agency finds that there are no grounds for overturning the local authorities' assessment that, as part of their selection of teaching and learning resources in primary and lower secondary schools, it is necessary to process and disclose personal data to Google in connection with the use of Google Chromebooks and Workspace for Education for the purposes of (i) the provision of and (ii) improving the security and reliability of the services in question, etc. ("the original purposes"), cf. Article 6(1)(e) of the General Data Protection Regulation, cf. Article 6(3), and sections 2(1) and 18(1) of the Primary and Lower Secondary Education Act. This includes, amongst other things, the processing of personal data for the purpose of providing the services, improving the security and reliability of the services, communicating with, amongst others, local authorities, and complying with legal obligations.

In this regard, the Danish Data Protection Agency has placed particular emphasis on the fact that the purposes in question are inextricably linked to Google's provision of Google Chromebooks and Workspace for Education to the local authorities, which must also be viewed in the light of technological developments and developments in how IT services are provided today.

The Danish Data Protection Agency also recognises that the further development of the teaching and learning resources which the local authorities have decided to use in primary and lower secondary schools is necessary to ensure that these resources reflect the present day, so that pupils can learn to deal with the issues and challenges of today and the future using up-to-date and modern tools.

However, it is the Danish Data Protection Agency's assessment that the local authorities cannot, within the framework of sections 2(1) and 18(1) of the Primary and Lower Secondary Education Act, cf. Article 6(1)(e) of the General Data Protection Regulation, process and disclose personal data relating to school pupils to Google as part of the use of Google Chromebooks and Workspace for Education for the purposes of (i) maintaining and improving the Google Workspace for Education service, Chrome OS and the Chrome browser, (ii) measuring the performance of Chrome OS and the Chrome browser, and (iii) developing new features and services in Chrome OS and the Chrome browser ('the secondary purposes').

The Danish Data Protection Agency hereby places particular emphasis on the fact that these secondary purposes cover not only the development of the specific teaching and learning resources procured by the local authorities, but also the general development of Google's products, such as Chrome OS and the Chrome browser. These products are not supplied exclusively to local authorities, but are generally available on the market; their further development therefore benefits, in the broadest sense, the market position of these products and the supplier. Furthermore, the Danish Data Protection Agency has emphasised that this development takes place on the basis of personal data relating to school pupils, which is collected as part of their use of the learning resources that they are required to use, regardless of whether this personal data is aggregated into general usage patterns.

Although it could be argued that this constitutes a less intrusive processing of personal data, given that the data is pseudonymised and aggregated – and therefore the requirements regarding the necessary legal basis are less stringent – and notwithstanding the flexibility which, in the Danish Data Protection Agency's view, is provided for in Article 6(1)(e) of the General Data Protection Regulation, and the 'necessity requirement' set out in that provision, the Danish Data Protection Agency considers that the relevant provisions of the Primary and Lower Secondary Education Act do not provide the necessary legal basis for local authorities to disclose information for the purposes in question.

It does not therefore appear, either from the wording of the Primary and Lower Secondary Education Act or from its preparatory works, that it is a necessary part of, or a prerequisite for, the local authorities' performance of their duties under the Act for them to disclose personal data on school pupils to the supplier of teaching and learning resources for the purpose of the supplier's general further development of its IT products through the use of such information. This does not follow either from a natural understanding of the Act's provisions on how IT was originally to be integrated into primary and lower secondary schools – and subsequently into individual subjects – or from the curriculum and teaching guidelines for the IT subject and its purpose.

It is therefore not apparent that it was the intention of the Folketing that the general further development of the teaching and learning resources which the local authorities decide to use in primary and lower secondary schools should be made possible by disclosing personal data on school pupils who use the teaching and learning resources in question to third parties, including the supplier thereof. Furthermore, there is absolutely no indication that the Folketing generally foresaw the technological developments that have taken place since the adoption of the relevant provisions of the Primary and Lower Secondary School Act in 1993.

The fact that KL, in addition to the Primary and Lower Secondary Education Act and the preparatory works thereto, has referred to the Joint Public Sector Digitalisation Strategy 2011–2015 and the 2012 financial agreement between the local authorities and the Government cannot lead to a different conclusion. None of these can be regarded as an expression of the legislature's intention regarding the tasks and obligations of the local authorities in relation to primary and lower secondary education, or how these are to be carried out.

Finally, the Danish Data Protection Agency notes that the considerations mentioned do not appear to be an isolated problem in relation to the Primary and Lower Secondary Education Act. The Danish Data Protection Agency therefore urges the legislator to take a clear stance in future on the extent to which personal data relating to citizens, as part of the social contract, may or must be disclosed in cases such as the one in question, including in particular in public-private partnerships.

The Danish Data Protection Agency therefore finds grounds to issue orders to the local authorities requiring them to bring their processing of personal data – in the form of the disclosure of personal data to Google – into compliance with Article 5(1)(a) and Article 6(1) of the General Data Protection Regulation, and to be able to demonstrate this, see Article 5(2) of the Regulation.

This may be achieved, for example, by:

the local authorities ceasing to disclose personal data to Google for the purposes in question, which is likely to require Google to develop a technical solution to block the relevant data flows, Google refraining from processing data for these purposes, or
the Danish Parliament providing a sufficiently clear legal basis for the processing in question.

The Danish Data Protection Agency initially requests that the local authorities state how they intend to comply with the above order. The Danish Data Protection Agency requests that this statement be submitted by 1 March 2024 at the latest.

The deadline for compliance with the order is 1 August 2024. The Danish Data Protection Agency requests that confirmation of compliance with the order be provided by that date at the latest. The order is issued pursuant to Article 58(2)(d) of the General Data Protection Regulation.

Under Section 41(2)(4) of the Data Protection Act, a person who fails to comply with an order issued by the Danish Data Protection Agency pursuant to Article 58(2)(d) of the General Data Protection Regulation is liable to a fine or imprisonment for up to six months.

5. Concluding remarks

In view of the nature of the case, the Danish Data Protection Agency has decided to inform the Parliament's Legal Affairs Committee and the Committee on Digitalisation and IT, as well as the Ministry of Justice and the Ministry of Children and Education, of the case.

As regards the other issues in the case, the Danish Data Protection Agency notes that it is continuing to examine these and expects to continue doing so in parallel with the local authorities' compliance with the aforementioned order.

[1] C-175/20, Valsts ieņēmumu dienests, paragraph 83.

[2] Consolidated Act No. 1086 of 15 August 2023 on primary and lower secondary education.

[3] The Digitalisation Strategy 2011–2015, including annexes, is available here: https://digst.dk/strategier/den-faellesoffentlige-digitaliseringsstrategi/tidligere-strategier/digitaliseringsstrategien-2011-til-2015/

[4] The Digitalisation Strategy 2011–2015, Focus Area 3 – Primary schools must challenge the digital generation, p. 22.

[5] Google has stated that the provision of personalised services "is a purpose under the Google Privacy Policy that applies to processing via Chrome Sync, except when the customer uses that service as part of Workspace for Education (in which case, the Google Privacy Policy, including this purpose, will not apply to that processing, and the Google Cloud Privacy Notice will apply instead). As we understand that all of the relevant Danish municipalities will use Chrome Sync as part of Workspace for Education, this processing purpose will not be applicable to their end users."

[6] See note 6.

[7] See the definition of 'Services' in clause 15.19 of the Google Workspace for Education Terms of Service

[8] See the definition of 'Chrome Services' in clause 15 of the Chrome Online Agreement.

[9] Google Terms of Service (dated 5 January 2022): https://policies.google.com/terms

[10] Google Privacy Policy (dated 4 October 2023): https://policies.google.com/privacy

[11] Google Privacy Policy (dated 4 October 2023): https://policies.google.com/privacy