DATATILSYNET

18 August 2022

The Danish Data Protection Agency upholds prohibition in Chromebook case

In a much-discussed case concerning the use of Google Workspace in Helsingør Municipality, the Danish Data Protection Agency has now considered the material most recently submitted by the municipality. On that basis, the Danish Data Protection Agency is upholding the ban imposed in July.

Summary

In a new decision, the Danish Data Protection Agency has upheld the processing ban on Helsingør Municipality's use of Google Workspace, which the Agency imposed in mid-July.

This follows a thorough review of the extensive material that Helsingør Municipality submitted to the Danish Data Protection Agency on 1 August. In the Danish Data Protection Agency's assessment, the municipality has still not demonstrated that it has mitigated the high risks posed to children in the municipality's schools.

"Teachers and pupils are currently in a difficult situation where they cannot use the tools they are accustomed to. Our decision in no way prohibits the use of IT in schools – but the specific use of certain tools in the municipality is not justifiable in terms of protecting children's data. And to put it bluntly, this is a consequence of the municipality's choices and omissions over several years," says Allan Frank, an IT security specialist and lawyer at the Danish Data Protection Agency, adding:

"The aim here is not to comply with some opaque bureaucracy, but to protect pupils' data. Under the GDPR, children are entitled to special protection. As adults, we are each free to choose which digital services we wish to use, but children simply have to use the tools that primary schools make available to them. It is therefore important that local authorities ensure that children's data is not used for purposes other than those permitted under the Primary and Lower Secondary Education Act – such as marketing, profiling or product development."

As in the previous decision, the ban applies only to Helsingør Municipality.

Key points of the Danish Data Protection Agency's new decision

- The Danish Data Protection Agency – like Helsingør Municipality – considers that several of the processing operations entail a high risk to those using Google Workspace.

- Helsingør Municipality is of the view that all relevant risks have been identified and addressed, but the Danish Data Protection Agency assesses that this is not the case. In the Danish Data Protection Agency's view, the municipality has not assessed the relevant risks set out in the contract with the supplier itself, nor other publicly known risk issues associated with the technology they have chosen. Furthermore, the risks identified by the municipality have not been sufficiently mitigated.
- Helsingør Municipality has assessed that Google acts solely as a processor; however, in the Danish Data Protection Agency's view, Google acts in several areas as an independent controller processing personal data for its own purposes. This is based, amongst other things, on the fact that, according to the municipality's own documentation, Google considers itself to be the controller in a number of areas.
- The Danish Data Protection Agency notes that the material provided by Helsingør Municipality does not meet the content requirements for an impact assessment. For example, the municipality has not assessed the relevant risks – not even for the processing operations described – and has only partially described the necessary security measures.
- The Danish Data Protection Agency has been unable to establish that Helsingør Municipality's data protection officer has indicated that they have any comments on the impact assessment.
- In summary, it is the Danish Data Protection Agency's assessment that Helsingør Municipality cannot reduce the risk to an acceptable level without changes to the contractual basis and the technology the municipality has chosen to use.

What can Helsingør Municipality do now?

If Helsingør Municipality wishes to continue using Google Workspace in its schools, it should, in collaboration with its suppliers, address the relevant risks to children's personal data – including those highlighted by the Danish Data Protection Agency in the three decisions – and prepare an impact assessment.

If the municipality acknowledges that it is not entirely possible to mitigate every high risk, the GDPR provides for the option of working with the Danish Data Protection Agency to draw up a plan to ensure compliance with the law.

The Danish Data Protection Agency is already proposing that the local authority and the Agency meet as soon as possible to discuss the next steps in more detail, so that pupils and teachers can return to a normal daily routine as quickly as possible in a responsible manner.

What about the other local authorities?

Although the decision specifically concerns the processing of personal data in Helsingør Municipality, the Danish Data Protection Agency urges other municipalities facing similar circumstances to examine the same areas as in this case – particularly with regard to disclosure without a legal basis and transfer to unsafe third countries. The task here is to assess whether there are similar issues in the individual local authorities and, if so, to work with the suppliers to bring the processing into line so that the equipment can be used in accordance with the rules.

Under the GDPR, it is the individual local authority that is the controller. However, the Danish Data Protection Agency encourages a collective approach, so that local authorities work together – possibly under the auspices of Local Government Denmark (KL) or the relevant line ministries – to resolve the issues. Many of the circumstances will be comparable or identical.

Although the local authorities are the controllers, the suppliers chosen by the local authorities also have an important role to play. They must help to document usage and amend the terms and conditions and technology where necessary. This applies to suppliers in general – but in this specific case, the Danish Data Protection Agency has also been in dialogue with Google and has directly urged the company to play an active role in finding solutions that can reduce the risk to children.

Decision

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

1.1. The decision of 10 September 2021

On 10 September 2021, the Danish Data Protection Agency issued a decision concerning Helsingør Municipality's personal data breach. The Danish Data Protection Agency found, amongst other things, that there were grounds for expressing serious criticism of the fact that Helsingør Municipality's processing of personal data through the use of Google Chromebooks had not been carried out in accordance with Article 5(2) of the General Data Protection Regulation[1], cf. Article 5(1)(c) and (f), and Article 5(1)(a), cf. Article 6(1), as well as Article 32(1), Article 33(1) and Article 35(1).

Furthermore, the Danish Data Protection Agency found grounds to issue an order to Helsingør Municipality to bring its processing of personal data through the use of Google Chromebooks into compliance with the General Data Protection Regulation. This was to be achieved by Helsingør Municipality carrying out, by 1 November 2021, a risk assessment of the processing activity that reflects the flows of personal data involved in the processing. The risk assessment was to address, on the one hand, the necessary options for configuring the product and, on the other hand, examine the legal basis in the Primary and Lower Secondary Education Act for the municipality's requirement that pupils use Google Chromebooks in schools. If the risk to the rights and freedoms of data subjects was assessed as high, the municipality was also required, as part of the order, to carry out an impact assessment. The order was issued pursuant to Article 58(2)(d) of the General Data Protection Regulation.

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

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

Following up on the Danish Data Protection Agency's decision of 10 September 2021, Helsingør Municipality, by letter dated 10 November 2021, submitted the municipality's risk assessment concerning the use of Google Chromebooks and G Suite for Education to the Danish Data Protection Agency; the municipality also submitted further documentation to demonstrate

the lawfulness of the processing activity. In response to a request dated 2 December 2021 from the Danish Data Protection Agency, Helsingør Municipality also submitted a range of further information on the case on 9 December 2021.

1.2. The decision of 14 July 2022

On 14 July 2022, the Danish Data Protection Agency issued a new decision concerning Helsingør Municipality's processing activities involving the use of Google Chromebooks and Workspace for Education. In this decision, the Danish Data Protection Agency found grounds to issue a prohibition to Helsingør Municipality against processing personal data using Google Chromebooks and Workspace for Education. The ban remained in force until Helsingør Municipality had brought its processing activities in to compliance with the General Data Protection Regulation – as stated in the decision – and had prepared adequate documentation to that effect.

Furthermore, in the decision, the supervisory authority suspended any transfer of personal data to the US that Helsingør Municipality had instructed Google Cloud EMEA Limited to carry out in its capacity as processor for the municipality, until Helsingør Municipality could demonstrate that the rules in Chapter V of the General Data Protection Regulation had been complied with.

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

The prohibition and suspension were imposed pursuant to Article 58(2)(f) and (j) of the General Data Protection Regulation.

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

2. Decision

Following up on the Danish Data Protection Agency's decision of 14 July 2022, Helsingør Municipality submitted a document entitled 'Impact Assessment for Google Chromebooks and G Suite for Education', together with annexes, to the Danish Data Protection Agency on 1 August 2022, including, amongst other things, a revised risk assessment.

Having reviewed and assessed the material submitted by Helsingør Municipality to the Danish Data Protection Agency on 1 August 2022, the Agency finds that Helsingør Municipality's processing of personal data through the use of Google Chromebooks and Workspace for Education remains non-compliant with the General Data Protection Regulation, including that the documentation dated 1 August 2022, prepared by Helsingør Municipality, does not comply with Article 35(1) and (7) and Article 36(1) of the General Data Protection Regulation.

Against this background, **the Danish Data Protection Agency's prohibition of 14 July 2022 is upheld.**

However, the prohibition is amended such that the Danish Data Protection Agency prohibits Helsingør Municipality from processing personal data using Google Chromebooks and

Workspace for Education. The prohibition shall apply until Helsingør Municipality has brought the processing activity into compliance with the General Data Protection Regulation, as set out in the Danish Data Protection Agency's decision of 14 July 2022, and has carried out a data protection impact assessment that meets the requirements regarding content and procedure for its implementation, as set out in Articles 35 and 36 of the Regulation. For processing operations where prior consultation with the Danish Data Protection Agency is required under Article 36 of the General Data Protection Regulation, the prohibition applies until the Agency has issued an opinion pursuant to Article 36(2), and Helsingør Municipality has taken the necessary measures on the basis of the Danish Data Protection Agency's opinion, or until the Agency authorises the processing at a time prior to the opinion being issued.

The prohibition, issued pursuant to Article 58(2)(f) of the General Data Protection Regulation, takes effect immediately.

Under Section 41(2)(4) of the Danish Data Protection Act[2], a fine or imprisonment for up to six months shall be imposed on any person who fails to comply with a temporary limitation or definitive restriction on processing issued by the Danish Data Protection Agency pursuant to Article 58(2)(f) of the General Data Protection Regulation.

The Danish Data Protection Agency further reserves the right to exercise additional powers under Article 58(2) of the General Data Protection Regulation in relation to the matters described in this decision, once Helsingør Municipality has submitted final documentation that fully clarifies the lawfulness of the processing operations and the risks to the rights and freedoms of data subjects. In addition, the above-mentioned circumstances may also be subject to sanctions under Section 41 of the Data Protection Act.

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

3. Statement of the case

Following the Danish Data Protection Agency's decision of 14 July 2022, Helsingør Municipality submitted new material in the case on 1 August 2022 in the form of the document 'Impact Assessment for Google Chromebooks and G Suite for Education' with four annexes:

1. Revised risk assessment
2. Settings for Google Chromebooks and G Suite for Education v. 1.0 dated 29 July 2022, applicable to one school in the municipality, and a copy confirming that identical settings had been established for all the municipality's schools
3. A package of documents comprising audit reports, contract terms, Google white papers and Google User Data Requests
4. A schematic overview of issues and the mitigating measures implemented

3.1. Comments from Helsingør Municipality

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

"Attached is the municipality's impact assessment, which addresses the issues raised. As an annex to the impact assessment, Annex 2 contains, amongst other things, a large number of screenshots documenting the municipality's settings. The total documentation comprises several hundred screenshots. However, due to the sheer number involved, the municipality has,

for the purposes of this submission, attached screenshots for just one school to illustrate these settings; however, should the Danish Data Protection Agency wish to receive all these screenshots, the municipality will be happy to provide them. […]

As the school year for the municipality's school-age children begins on 8 August 2022, and as the use of the Services is an essential prerequisite for delivering the planned teaching in the 2022/2023 school year, it is naturally of great importance to the municipality that the ban be lifted. […]

For the sake of clarity, it should be noted that although the municipality's pupils will start the new school year on **8 August 2022**, the municipality will not issue computers or grant access to the Services to new pupils in Year 0. […]"

The Helsingør Municipality document 'Impact Assessment concerning Google Chromebooks and G Suite for Education' of August 2022 states, amongst other things, the following:

"Description of the processing activities

1. Nature, scope, context and purpose of the processing

For teaching purposes, a digital learning platform based on Google Chromebooks with Workspace for Education Standard is used. The platform enables the sharing of documents between pupils and teachers and generally facilitates collaboration within the class and across classes.

Information contained in the Services relates to pupils and teachers.

As a general rule, no sensitive information, Danish civil registration (CPR) numbers or information about criminal offences relating to pupils or teachers is processed via the systems. However, it cannot be ruled out that such information may be included in emails from teachers or in other material, and instructions have also been given to teachers to prevent this. This must therefore be regarded as highly unusual and unintentional.

This concerns personal data relating to pupils, who generally enjoy special protection under data protection rules, as pupils of compulsory school age are considered a vulnerable group of individuals given their age.

Helsingør Municipality works purposefully to prepare children and young people for the society and labour market of the future as part of the municipality's remit to provide education. All year groups work with IT on a daily basis as an integral part of teaching across all subjects, in order to support subject-specific learning and pupils' digital skills, which underlines the necessity of this processing.

To ensure that schools and pupils have a forward-looking, sustainable model for IT-supported teaching, the municipality has chosen 'Tjenesterne' as its teaching platform.

2. Personal data, recipients and the period for which personal data is retained

The following types of personal data are processed, in the following manner, to fulfil the educational remit.

- Personal data: Name, Unilogin, class, email address (username, Unilogin + domain), school, material produced, emails sent and images (profile pictures or in material).
- Recipients Internally: Teachers, administrators, pupils. Externally: Wizkids and Google as processors
- Retention period Data is retained until a pupil either moves to another local authority or for three months after the pupil leaves school upon completion of their education (cell J9 in the risk analysis).

3. Systematic description of the processing activity

KL describes the general processing activity for the school sector as follows:

"The processing of personal data is carried out for the purpose of organising the school year, including pupil assessments, well-being surveys, claims for compensation from pupils and pupil statements.

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

Furthermore:

For teaching purposes, a digital learning platform based on Google Chromebooks with Workspace for Education Standard – the Services – is used. The platform enables the sharing of documents between pupils and teachers and generally facilitates collaboration within the class and across classes.

From 'cradle to grave', this can be systematically presented as follows:

1. Management of physical hardware
a) Purchase of a physical computer/Chromebook
b) Handover to pupil/parents
c) Return from pupil/parents
d) Re-issuing (after power wash)/disposal
2. Account creation and administration for the local authority's main Google account
a) Account creation and configuration (e.g. where data is stored)
b) Selection of facilities (core only)
c) Backup
d) Activity logging (pupils, teachers and admins)
3. User management and system monitoring
a) Creating classes (automatically via TEA)
b) Creation of pupils (automatically via TEA)
c) Creation of aliases for pupils with name protection (manually; until then, they remain in a pending status).
d) Reporting on pupils' and teachers' use of GWfES
e) When a pupil leaves Helsingør Municipality's state school, this is recorded in TEA and the pupil's data is deleted after 3 months (automatically)
4. Teacher activities
a) Creation and storage of lesson plans, assignments and questionnaires (Classroom, Drive)
b) Marking of assignments (Classroom, Drive)
c) Chat (Hangouts, Meet)

5. Pupil activities
a) Creating and saving assignments (Drive), reading lesson plans
b) Writing and submitting assignments and reading feedback
c) Chat (Hangouts, Meet)
d) The assets on which the personal data depends (hardware, software, network, people, paper, paper-based delivery channels) are identified.

- Chromebook (the browser acts as a 'client' for the cloud solution)
- Workspace for Education Standard (configured as a European data centre) (part of the cloud solution)
- Google's data centre (part of the cloud solution)
- School network
- Admins (the local authority's IT school support staff)
- Wizkids
- School secretaries (TEA pupil administration platform, aliases)
- Teachers
- Pupils

Risk assessment and description of measures to address these risks

The risk assessment prepared is attached as **Annex 1** to this impact assessment under the headings 'privacy by design' and 'use of data for unintended purposes'. Documentation of the mitigating measures implemented is attached as **Annexes 2 and 3.**

Lawfulness and the rights of data subjects

1. Lawfulness of processing

[…]

It is apparent from the Danish Data Protection Agency's decision of 14 July 2022 that the local authority has not sufficiently safeguarded Google's role as a processor in relation to Google's access to personal data, including in particular through the ordinary use of the Google Chromebook operating system and Google Workspace's interaction with Google's backend, and that the local authority has not provided the necessary guarantees that Google will comply with the requirements of the General Data Protection Regulation, cf. Article 24 of the Regulation, cf. Article 28(1).

It is the municipality's assessment that the measures described in the risk assessment drawn up in October 2021 will normally be sufficient to demonstrate that Google acts solely as a processor and in accordance with this role.

It should be noted that the municipality is not, moreover, aware of any practice on the part of the Danish Data Protection Agency which, in other cases, requires similar documentation in relation to the use of a processor that does not have a 'history' of acting outside the scope of the processor role.

In the Danish Data Protection Agency's decision of 14 July 2022, this critical stance towards Google as a processor is, as far as the municipality can assess, not substantiated in any further detail. However, following the decision, the Danish Data Protection Agency has stated orally that practice in the Netherlands casts doubt on whether Google processes personal data from

the Services in the education sector for its own commercial purposes, which are irrelevant and unjustified in relation to the use of the Services in this sector.

The local authority has therefore, as part of its work on this impact assessment, also provided information on the points of criticism levelled against Google in the Dutch case[3]. Specifically, these relate to the following overarching issues as at February–March 2021:

- Lack of purpose limitation of Customer Data
- Lack of purpose limitation of Diagnostic Data
- Lack of transparency regarding Customer Data
- Lack of transparency regarding Diagnostic Data
- Lack of legal basis for Google to process personal data as a controller
- Lack of control over the way in which Google processes personal data
- Lack of control over the processing of personal data by Google's subcontractors
- Lack of opportunity for data subjects to access their data

The local authority understands the Dutch DPIA to mean that these issues essentially concern challenges arising from the fact that Google was, in whole or in part, the controller; that Google demanded the right to process personal data as a processor as part of its services for purposes which were difficult to reconcile with the Services; and that the processing of personal data, amongst other things, cookie and telemetry data involved processing that was non-transparent.

For the sake of completeness, the municipality has, in Annex 4, assessed a number of issues raised in the Dutch case. This review shows that these issues are of very limited relevance to Helsingør Municipality's use of the Services, as the roles and set-up are fundamentally different. A key reason for this is, amongst other things, that the municipality uses only the Core Services, and that Google therefore acts solely as a processor and thus processes personal data solely for the municipality's purposes. Google has unequivocally acknowledged this role in this case (including in the data processing agreement and the attached documentation in Annexes 2 and 3), together with the limitations that follow from it.

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

The municipality has therefore chosen to focus the mitigating measures on documenting that Google is solely a processor and processes personal data solely as a processor for the purposes set out in the municipality's instructions when Google processes personal data as a processor on behalf of the municipality.

A more schematic overview of the potential issues identified in the Dutch decision and the associated DPIA, together with details of how Helsingør Municipality has mitigated these issues, is set out in Annex 4 to this impact assessment.

These mitigating measures are as follows:

- Documentation is attached to show that the municipality has selected settings which ensure that the municipality uses only Core Services, see Annex 2. These settings mean that Google acts solely as a processor and that Google may only act in

accordance with the municipality's instructions and is therefore not legally permitted to pursue its own purposes.

- Documentation has been obtained in the form of independent third-party statements confirming that Google, as a processor, does not pursue its own purposes, see Annex 3. This documentation ensures that an independent third party has audited Google's processing of personal data in its capacity as a processor, and thereby that Google, as a processor, acts within the given instructions and does not pursue its own purposes in breach of the data processing agreement.
- This impact assessment provides an overview of the investigations and considerations carried out by the local authority in response to the issues raised, and assesses whether, in light of the above, the processing entails a high risk.

The risk assessment shows that, in relation to the rights and freedoms of data subjects, the processing – with these mitigating measures in place – presents a medium risk, which the local authority can accept. It should be noted in this regard that the risk is scored at 8, which is the lowest score in the medium-risk category. It is further noted that the primary reason the risk is not lower is that the processing concerns data relating to school pupils of compulsory school age, and that children enjoy special protection under data protection legislation. The risk to school pupils has thus been mitigated to an acceptable level.

It is therefore the municipality's overall assessment that the two risks identified in the Danish Data Protection Agency's decision have been mitigated to an appropriate and acceptable level.

2. Basic conditions and lawful processing

In order to process personal data in the Services as part of fulfilling its statutory educational duty, the local authority must have a legal basis for the processing of personal data.

Although it follows from the Primary and Lower Secondary Education Act that the municipality must provide education to children of compulsory school age – and the processing of personal data is a prerequisite for this – it is the municipality's assessment that the Primary and Lower Secondary Education Act does not, on its own, constitute the legal basis for this processing, but rather the actual legal basis.

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

This intended processing is carried out to fulfil tasks in the public interest and as part of the exercise of official authority entrusted to the local authority (the duty to provide education). This means that Article 6(1)(e) of the General Data Protection Regulation constitutes the legal basis for the processing of personal data in the Services.

With regard to the principles governing the processing of personal data, the Danish Data Protection Agency has stated that the local authority has not demonstrated that the processing is lawful, fair and transparent. According to the decision, this is because the local authority

- has not included in its risk assessment the risk scenarios that may arise as a result of the data processor arrangement and the system choices made
- has not carried out sufficient testing of the scope and functioning of the selected hardware and the software used

- cannot document how the local authority controls Google's access to personal data, including, in particular, during normal use of the Google Chromebook operating system and Google Workspace's interaction with Google's backend in relation to the possibilities for separating personal data that may arise under the [data processing agreement]

As stated above, a detailed explanation has been provided as to why these issues are of limited relevance in this case. As also noted, the local authority has furthermore attached documentation which describes in detail why, in the local authority's assessment, Google does not have a realistic opportunity to blur the line between its role as a processor and Google's own purposes, which differ from the provision of services to the local authority, see Annexes 2 and 3.

The local authority understands the applicable law to mean that contractual obligations may also constitute mitigating measures. For the sake of completeness, the local authority would therefore also like to refer to the data processing agreement with Google[4], which states the following:

"5.2 Scope of Processing.

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

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

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

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

As previously described, the local authority does not use the Additional Services, and the data processing agreement is therefore very clear in that Google acts solely as a processor, and that Google may only process personal data for the local authority's purposes.

The totality of mitigating measures in the form of the data processing agreement with Google, the municipality's settings, etc., see Annex 2, Google's supplementary documentation, see Annex 3, and the assessment of the relevance of the Dutch case, to which the Danish Data Protection Agency has referred, see Annex 4, means that, in the municipality's assessment, there is sufficient documentation to demonstrate that the processing is lawful, fair and transparent.

In this connection, the municipality further notes that this documentation must not be assessed in a vacuum. The fact that the Services are undoubtedly covered by the scope of the General Data Protection Regulation and the Danish Data Protection Agency's jurisdiction, the obligations agreed upon by Google under the data processing agreement and the municipality's instructions, and Google's documentation demonstrating that it complies with these obligations, taken together with a more general contractual obligation on Google towards the municipality, means that, overall, Google would expose itself to a very high risk of fines and claims for damages were it to process data in breach of these obligations.

In addition to the principle of lawful processing, the local authority would also like to draw particular attention to the principle of data minimisation. In the risk assessment, this is addressed as a separate issue in row 11, and it is the local authority's assessment that this principle is also being complied with.

3. The rights of data subjects

The local authority has drawn up privacy policies and procedures which help to safeguard the rights of data subjects. The local authority therefore informs data subjects about the processing. In addition to the information in the privacy policy on the website, the local authority will send a further information letter to staff.

The local authority also has procedures in place for handling requests for access to data, as well as requests from data subjects for rectification and erasure, etc. These procedures ensure that the local authority responds to a request from a data subject without undue delay and within one month at the latest, unless the request is complex, in which case the response deadline may be extended by a further two months.

Particularly with regard to the handling of requests from data subjects, the local authority's procedures are supported by the data processing agreement with Google, which states the following:

"9.2 Data Subject Requests.

9.2.1 Responsibility for Requests. During the Term, if Google's Cloud Data Protection Team receives a request from a data subject that relates to Customer Personal Data and identifies Customer, Google will: (a) advise the data subject to submit their request to Customer; (b) promptly notify Customer; and (c) not otherwise respond to that data subject's request without authorization from Customer. Customer will be responsible for responding to any such request including, where necessary, by using the functionality of the Services.

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

providing Additional Security Controls in accordance with Section 7.1.3 (Additional Security Controls);
complying with Sections 9.1 (Access; Rectification; Restricted Processing; Portability) and 9.2.1 (Responsibility for Requests); and
if subsections (a) and (b) above are insufficient for Customer (or the relevant controller) to comply with such obligations, upon Customer's request, providing Customer with additional reasonable cooperation and assistance."

It is against this background that the local authority assesses that the use of the Services will be able to safeguard the rights of data subjects. […]

Monitoring and updating

The impact assessment shall be reviewed at least once a year, and shall also be reviewed if, based on a risk-based approach, it is assessed that there may be significant changes relating to the processing activities covered.

The views of data subjects

As part of the impact assessment, the controller must, where relevant, seek the views of data subjects or their representatives. These views may be obtained by various means, depending on the situation. It is up to the controller to decide how this should be done. For example, focus groups, questionnaires, consultation with staff representatives or consultation with a relevant organisation may be used. If the controller's final decision differs from the views of the data subjects, the authority's or organisation's reasons for proceeding or not must be set out.

This impact assessment is based specifically on a complaint from a parent and the decisions of the Danish Data Protection Agency. Helsingør Municipality has therefore not, on the basis of a professional assessment, deemed it relevant to seek further views from the data subjects or their representatives.

Submission to the DPO

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

[…]

Appendix 3 – Documentation showing that Google, as a processor, does not pursue its own purposes

1. ISO 27001 certification

Google is ISO 27001-certified[5]. This certification of Google as an organisation entails a requirement that Google complies with applicable legislation and requirements. This includes, amongst other things, the following

- *Clause 4.2 Understanding of stakeholders' needs and expectations, where subclause (b) states that the organisation must determine stakeholders' requirements relevant to information security. The local authority adds that this also covers requirements relating to contracts entered into, as detailed below.*

- *Annex A: A5.1 Guidelines for information security management, which states that the purpose is "to provide management direction and support for information security in accordance with business requirements and relevant laws and regulations".*
- *Annex A: A18.1 Compliance with legal and contractual requirements, which states that the purpose is "to avoid breaches legal, statutory, regulatory or contractual obligations relating to information security and of any security requirements".*

The aforementioned requirements must be complied with in order to meet the conditions for obtaining certification.

2. Google's supplementary guarantees and information, set out below:

Customer Questions	Google Responses
1) Can Google guarantee that, when acting as a data processor for Helsingør Municipality, it does not process Customer Data or other personal data for – for which Helsingør Municipality is the data controller – for marketing purposes?	Our customers' data belongs to them, not to Google. Google only processes Customer Data in accordance with the contracts with customers, and specifically undertakes in the Google Workspace for Education Terms of Service that Google does not process Customer Data for its own purposes, including for advertising purposes. Google's commitment to process Customer Data solely in accordance with customer contracts and for no other purpose is also subject to audit by an independent third-party auditor (currently, EY). For example, Google's latest SOC 2 report describes various tests carried out by EY regarding Control 22, which states: "The organisation only processes customer data in accordance with the applicable data processing terms and does not process customer data for any other purpose", with no deviations noted. Please see our response to question 6 for further instructions on how to download our SOC 2 report and other compliance-related resources. For users in primary and secondary schools, Google does not use any user personal information (or any information associated with a Google Workspace for Education account) to target advertising, whether in Google Workspace Core Services (such as Gmail or Calendar), Chrome Education Upgrade, or other Google services accessed whilst using a Google Workspace for Education account.
2) Can Google confirm that, when the settings in Google Workspace and Google Chromebooks are configured to ensure that only Core Services are used and available, and that Additional Services are disabled, Google will only process personal data in its capacity as a data processor and not for any purposes other than those specified by Helsingør Municipality?	When Additional Services are disabled and only Workspace Core Services are used: • Google processes Customer Personal Data as a data processor and only in accordance with your instructions. As mentioned in our response to question 1, we do not process Customer Data (including Customer Personal Data) for our own purposes (including advertising purposes), and this commitment is

	subject to audit by our independent third-party auditor. • Google processes Service Data as a controller for limited purposes in accordance with our Google Cloud Privacy Notice. As set out in our Notice, Service Data is the personal information we collect or generate whilst providing and administering the Google Workspace services, excluding Customer Data. We have provided further details on the purposes for which we process Service Data in our response to question 3 below.
3) Does Google, as a data processor, process Diagnostic Data – including telemetry, cookies, etc. – for purposes other than those specified by Helsingør Municipality?	If "Diagnostic Data" (as described in your question) contains personal data, then it is classified as "Service Data" when it has been collected or generated through the Workspace Core Services. Google may process this Service Data as a data controller for the limited purposes described in the section 'Why we process data' of the Google Cloud Privacy Notice.
4) When Google provides online technical support, can such support be initiated by Google on its own initiative, or will it only be initiated at the request of Helsingør Municipality?	We understand "online technical support" to refer to our Technical Support Services for Google Workspace. As explained in our Google Workspace Subprocessors URL, Technical Support Services are "customer-initiated" and would not be initiated by Google, as, by their very nature, Technical Support Services depend on a request from a customer. This article describes how your administrator can contact Google directly for support.
5) Will it in the near future be possible, as a general Google feature, to opt out of online technical support from non-secure third countries?	Firstly, we would like to clarify that every sub-processor we engage undergoes a rigorous selection process to ensure it possesses the necessary technical expertise and can deliver the appropriate level of security and privacy. We provide the same contractual commitments for all sub-processors in Section 11 of our Data Processing Amendment. As noted in our response to question 4, we understand 'online technical support' to refer to our Technical Support Services for Google Workspace. Google continues to invest heavily in features designed to offer enhanced control over the geographical location of data. At present, in order to provide 24/7 Technical Support Services as part of the 'follow the sun' support model, these services may be provided from locations outside the EU/EEA. However, as stated in our Google Workspace Subprocessors URL: · Each Third-Party Sub-processor providing Technical Support Services "only has access to Customer Data if the

	Customer explicitly elects to share Customer Data in the course of a support case (e.g. screen shots)". · Google Group Sub-processors providing Technical Support Services "may require limited, authorised access to Customer Data to respond to requests initiated by the Customer". Our customers can rely on our Standard Contractual Clauses (as well as our supplementary measures) as a legal mechanism to meet their compliance requirements regarding the transfer of Customer Personal Data (i.e. the personal data contained within Customer Data) outside the EU.
6) Where possible, Helsingør Municipality would appreciate any documentation, including documentation from third parties such as audits, etc., to support the answers provided above.	**Compliance Resources** Our Compliance Reports Manager provides you with easy, on-demand access to critical compliance resources. Please go to https://cloud.google.com/security/compliance/compliance-re-ports-manager/ and sign in with your Google Workspace account to view all the resources available to you. You may wish to review the following in particular: • ISO certification (27001, 27017, 27018, 27701) * SOC 1, 2 and 3 audit reports As indicated above, we are also compiling other talking points and resources that may be useful in supporting your Data Protection Impact Assessment. We will share these with you early next week. **Other Useful Resources: Chromebooks** 1. ChromeOS 1-Pager 2. ChromeOS (ISO 27001, 27017/18, SOC1) * Chrome Enterprise Upgrade * Chrome Education Upgrade * Chrome Non-profit Upgrade * Chromebook Enterprise Our guide on how to customise and implement Google Workspace (including best practices for privacy) 1. Google Workspace for EDU data protection implementation guide Data Processing Terms & Customer Data Processing Commitments 2. Google Workspace Service-Specific Terms 3. Data Processing Amendment to the Google Workspace and/or Complementary Product Agreement 4. Google's adherence to the EU GDPR Code of Conduct Service Data 5. Google Cloud Privacy Notice 6. Google's commitment regarding the processing of Service Data Data Transfers and the Schrems II ruling 7. Transfer Impact Assessment: How to Assess the Risk of Cloud EEA–US Data Transfers Using the European Data Protection Board's Recommendations (the document has been omitted as Google considers the document in its entirety to be confidential)

8. Google Cloud's implementation of the New EU Standard Contractual Clauses
9. Safeguards for international data transfers with Google Cloud
10. Reaffirming Google Cloud's commitments to EU businesses in light of the EDPB's Recommendations
11. Google Cloud welcomes the EU's new Standard Contractual Clauses for cross-border data transfers

Additional Privacy Resources

12. Privacy Resource Centre
13. Google Transparency Report
14. Enhancing our privacy commitments to customers (blog post 2020)

Lack of purpose limitation for customer data

Potential issues	**How has Helsingør Municipality mitigated the risk?**
Google does not wish to expressly exclude the further processing of Helsingør Municipality's personal data in the role of ' ' as an independent controller for the purpose of detecting unlawful activity without first obtaining prior written authorisation from the Customer. Google does not provide controls to override or prevent scanning, filtering or other analysis of spam and malware, where this is commercially, technically and reasonably feasible.	Google acts solely as a processor, as the local authority only uses Core Services, and Google is and is therefore not a controller. This issue is not relevant. (This is confirmed, amongst other things, by the data processing agreement and by the ISO 27001 certification.) Pupils do not have access to the email function. Monitoring of teachers' use of email is enabled, including checks to ensure that attached files are not malicious and that incoming emails with attachments are opened in a sandbox. This issue is not relevant.
Google processes personal data as an independent controller for the purposes of marketing, profiling, data analysis and market research.	The risk is mitigated as Google has contractually undertaken not to process data for these purposes, given that the local authority uses only Core Services, cf. clause 5 of the data processing agreement.
There is a risk that machine learning used to improve the content of spelling and grammar data is not restricted to Helsingør Municipality's own domain	The municipality is the controller, i.e. the processing of texts etc. is carried out for the municipality's purposes. Furthermore, metadata reporting has been disabled, so Google has access to identifiable personal data in connection with machine learning.

When Google anonymises information and subsequently uses it, the anonymisation is not sufficient.	Google has stated that anonymisation is carried out as prescribed in the WP29 guidelines.

Lack of purpose limitation for diagnostic data

Potential issues	**How has Helsingør Municipality mitigated the risk?**
Google processes diagnostic data (including telemetry data), support data, feedback data and all settings/configurations selected by Enterprise customers for a wide range of its own purposes.	Diagnostic data and feedback have been disabled, as documented in Appendix 2.
Google does not follow the recommended measures to include Chrome Enterprise in the G Suite Enterprise offering or to include a separate Chrome browser with 'processor' mode on Android devices and Chromebooks (where it is not realistic to install another browser).	Google is solely the processor, as the local authority only uses Core Services, and Google is therefore not the controller. This issue is not relevant. (This is confirmed, amongst other things, by data processing agreements and the ISO 27001 certification.)

No legal basis for Google

Potential issues	**How has Helsingør Municipality mitigated the risk?**
Google does not wish to act as a processor for diagnostic data, support data and feedback data.	Google is the processor, and diagnostic data and feedback have been disabled, as documented in Appendix 2.
With regard to the legal basis for the collection of cookie and telemetry data from end-user devices, Google states that it uses cookies and similar technologies that are necessary for the services to function.	Diagnostic data and feedback have been disabled, as documented in Annex 2. Furthermore, Google acts solely as a processor, and the legal basis is therefore determined by the local authority.

Default settings for the protection of personal data that do not promote integrity

Potential issues	**How has Helsingør Municipality mitigated the risk?**

It is not possible to change Google's default settings, meaning that Helsingør Municipality cannot protect personal data via 'privacy by default'.	The municipality's choice of settings promotes 'privacy by design', as documented in the risk assessment and the attached documentation on settings, and the municipality considers the available setting options in the Services to be sufficient, see Appendices 1 and 2.

Lack of control over sub-processors	
Potential issues	**How has Helsingør Municipality mitigated the risk?**
It is not possible to monitor Google's sub-processors through audits or similar measures.	Google acts as the data processor for Helsingør Municipality in this matter, and the municipality supervises Google as the data processor and, to the extent necessary, its sub-processors in accordance with its internal procedures for this purpose. Overall, the municipality considers that the data processing agreement provides sufficient scope for this.

Lack of insight into personal data	
Potential issues	**How has Helsingør Municipality mitigated the risk?**
There is a risk that Google will not provide the necessary access to the personal data contained in telemetry and cookie data.	Diagnostic data and feedback have been disabled, as documented in Annex 2. Furthermore, Google acts solely as a processor, and the legal basis is therefore determined by the local authority. It should also be noted that, in the data processing agreement, Google has undertaken to assist in responding to requests for access. "

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

The Danish Data Protection Agency notes, first of all, that in this decision, the Agency has not taken a position on whether Helsingør Municipality has breached the prohibition imposed on the municipality by the Agency's decision of 14 July 2022.

This decision solely addresses whether – and, if so, to what extent – Helsingør Municipality has, through the documentation submitted, demonstrated that it can carry out the processing activity in accordance with data protection rules.

4.1. Relevant rules

It follows from Article 35(1) of the General Data Protection Regulation that the controller must, prior to any processing activity, carry out an analysis of the impact of the intended processing activities on the protection of personal data. This applies if the processing, in particular where new technologies are used and by virtue of its nature, scope, context and purposes, is likely to result in a high risk to the rights and freedoms of natural persons.

It also follows from Article 35(2) of the Regulation that the controller must consult the data protection officer, if one has been appointed, when carrying out a data protection impact assessment. This provision is naturally linked to Article 39(1)(c) of the Regulation, which states that the data protection officer's tasks include, as a minimum, advising on the impact assessment and monitoring its implementation when requested to do so in accordance with Article 35.

Article 35 of the General Data Protection Regulation also sets out a number of minimum requirements that a data protection impact assessment must meet. These requirements are set out in paragraph 7 of that provision and include:

a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and
d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

Furthermore, Article 35(11) of the General Data Protection Regulation states that the controller must, at least where there is a change in the risk posed by the processing operations, assess whether it is necessary to carry out a fresh review to determine whether the new processing is covered by impact assessments already carried out.

Finally, Article 36(1) of the Regulation states that the supervisory authority must be consulted prior to processing if a data protection impact assessment shows that the processing will result in a high risk in the absence of measures taken by the controller to mitigate that risk.

If, by carrying out the impact assessment – and taking the necessary measures – the controller has thus been unable to reduce the risk to a level lower than high, the Danish Data Protection Agency must be consulted before the processing commences. This is to ensure, on the one hand, the lawfulness of the processing and, on the other, that the controller has identified the relevant risks to data subjects and mitigated those risks. In this context, the Danish Data Protection Agency advises the controller on whether all relevant risks have been identified and, where appropriate, what measures the controller may take to mitigate those risks. In this connection, the Danish Data Protection Agency may exercise all its powers.

This therefore constitutes a significant legal safeguard for the rights and freedoms of data subjects. The disregard of this safeguard undermines the Danish Data Protection Agency's – as the competent supervisory authority – ability to become aware of and monitor the lawfulness

of high-risk processing operations and thus entails a risk of infringement of the rights and freedoms of data subjects.

The provisions of the General Data Protection Regulation (GDPR) on impact assessments and any consultation with the Danish Data Protection Agency are intended to ensure that no processing involving an inherent high risk to the rights and freedoms of data subjects is initiated without the controller having addressed and mitigated such risks.

A data protection impact assessment is thus a tool that enables the controller to address the risks that a processing activity may entail in a systematic manner.

A comprehensive description of the processing activity, see Article 35(7)(a), is a prerequisite for the controller to be able to assess and document the lawfulness of the processing activity, see paragraph 7(b).

Similarly, the factual circumstances relating to the processing activity and its lawfulness are a prerequisite for assessing any risks in the form of deviations from the intended, lawful processing activity, see paragraph 7(c).

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

The Danish Data Protection Agency may also refer to the guidance on impact assessments issued by the Agency and the Ministry of Justice in March 2018, which is available on the Danish Data Protection Agency's website. Furthermore, in October 2017, the European Data Protection Board adopted its 'Guidelines on the data protection impact assessment' (DPIA) and determining whether the processing 'is likely to result in a high risk' under Regulation (EU) 2016/679', which is also available on the Danish Data Protection Agency's website in a Danish version.

4.2. Processing operations that present a high inherent risk

On 10 September 2021, the Danish Data Protection Agency issued an order to Helsingør Municipality to bring the municipality's processing of personal data through the use of Google Chromebooks and Workspace into compliance with data protection rules. If it transpired that the risk to the rights and freedoms of data subjects associated with this was high, the municipality would also be required to carry out a data protection impact assessment.

On 10 November 2021, Helsingør Municipality submitted its risk assessment to the Danish Data Protection Agency in order to demonstrate that it had brought its processing activities into compliance with data protection rules. In this connection, Helsingør Municipality stated that it was the municipality's assessment that it was not obliged to carry out a data protection impact assessment, as the municipality did not use Google Workspace Add-on Services.

On 14 July 2022, the Danish Data Protection Agency issued Helsingør Municipality with a prohibition on processing personal data using Google Chromebooks and Workspace until the municipality had brought its processing activities into compliance with the General Data Protection Regulation as set out in the decision, and had prepared adequate documentation to that effect.

In this regard, the Danish Data Protection Agency emphasised that Helsingør Municipality had not fully assessed and documented the risk scenarios that could arise as a result of using

Google as a supplier and Google Chromebooks and Workspace as a system. The Danish Data Protection Agency also emphasised that the risk scenarios which the municipality had, however, assessed and documented indicated that there was likely to be a high inherent risk associated with the processing activity in question.

In this connection, the Danish Data Protection Agency based its decision of 14 July 2022 on the fact that Helsingør Municipality did not use Google Workspace Add-on Products. The Danish Data Protection Agency continues to base its assessment on this – in accordance with the information provided by Helsingør Municipality.

In its description of the processing activity, as set out in section 3.1 above, Helsingør Municipality has stated that Google Chromebooks and Workspace are used in teaching across all year groups, and that a range of specified personal data concerning, amongst others, pupils is processed. In the Danish Data Protection Agency's view, this therefore constitutes the same processing activity that is also the subject of the Agency's decisions of 10 September 2021 and 14 July 2022.

It is therefore – as also stated in the Danish Data Protection Agency's decision of 14 July 2022 – the Agency's assessment that Helsingør Municipality's processing of personal data through the use of Google Chromebooks and Workspace is likely to entail an inherently high risk to the rights and freedoms of natural persons.

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

The Danish Data Protection Agency notes, in this regard, that a processing activity such as this involves two of the nine factors which, according to the guidelines of the European Data Protection Board[6], indicate a high inherent risk. Furthermore, it is the Danish Data Protection Agency's view that Helsingør Municipality's specific use of Google Chromebooks and Workspace involves a third factor indicating a high risk, namely that it involves extensive processing of personal data, as the hardware and software in question are used across the municipality's primary schools.

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

This is also set out in the Danish Data Protection Agency's decision of 14 July 2022. In this connection – as an indication that the processing activity is likely to present a high risk – the Danish Data Protection Agency has assessed in more detail the extent to which information for which Helsingør Municipality is the controller is processed for purposes other than those provided for in the Primary and Lower Secondary Education Act.

The Danish Data Protection Agency has stated the following in this regard:

"It is the Danish Data Protection Agency's view that Helsingør Municipality's processing of personal data under the Primary and Lower Secondary Education Act, cf. Article 6(1)(e) of the Regulation, does not cover situations where personal data is processed for purposes other

than those provided for in the Primary and Lower Secondary Education Act. Consequently, the data may not lawfully be disclosed to other controllers for their own purposes where such purposes are not provided for in the Primary and Lower Secondary Education Act. This also includes the processing of personal data that may occur through pupils' use of the equipment and software, including metadata used for marketing and profiling, regardless of whether the data is used for direct marketing and profiling or indirectly as part of a group (class, year group, school, etc.)."

It is therefore the Danish Data Protection Agency's assessment that the processing activity in question generally – due to the presence of three overarching factors indicating that the processing activity is likely to entail a high risk, and in light of the specific risk scenario concerning the processing of personal data for other purposes – requires Helsingør Municipality to carry out a data protection impact assessment, cf. Article 35 of the Regulation.

In conclusion, the Danish Data Protection Agency notes that it is stated in the guidance on impact assessments issued by the Danish Data Protection Agency and the Ministry of Justice in March 2018, that it is not necessary to carry out a data protection impact assessment for activities that were ongoing at the time the General Data Protection Regulation became applicable and which were inspected by the Danish Data Protection Agency pursuant to the rules on the duty to notify set out in Chapters 12 and 13 of the then-applicable Personal Data Act.

However, it is also stated that, should there be a change to the processing activity, the controller must assess whether an impact assessment is required under the provisions of the General Data Protection Regulation. This must be read in conjunction with Article 35(11) of the General Data Protection Regulation, under which the controller is obliged to assess on an ongoing basis whether changes to the processing activity give rise to a need to review an existing impact assessment, at least where there is a change in the risk posed by the processing activities.

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

It is generally the Danish Data Protection Agency's view that substantial changes to terms and conditions, software and applications usually constitute a significant change to the risk posed by the processing activity.

Although the processing activity in question commenced before 25 May 2018, it is therefore the Danish Data Protection Agency's view that Helsingør Municipality's obligation to carry out a data protection impact assessment under Article 35 of the General Data Protection Regulation was triggered after the Regulation became applicable, and that Helsingør Municipality has been obliged to keep this data protection impact assessment up to date on an ongoing basis.

4.3. Helsingør Municipality's documentation of 1 August 2022

On 1 August 2022 – in response to the Danish Data Protection Agency's decision of 14 July 2022 – Helsingør Municipality submitted its documentation concerning the municipality's use of Google Chromebooks and Workspace.

The documentation states, amongst other things, that it has been prepared solely on the basis of the Danish Data Protection Agency's decision of 14 July 2022, and that the documentation is intended to address the risks which the Agency addressed in its decision of 14 July 2022.

It is stated below that, in order to address the issues raised by the Danish Data Protection Agency, Helsingør Municipality has taken the following steps:

"Documentation is attached to show that the municipality has selected settings which ensure that the municipality uses only Core Services, see Annex 2. These settings mean that Google acts solely as a processor and that Google may act only within the municipality's instructions and thus cannot lawfully pursue its own purposes.

Documentation has been obtained in the form of independent third-party statements confirming that Google, as a processor, does not pursue its own purposes, see Annex 3. This documentation ensures that an independent third party has audited Google's processing of personal data in its capacity as a processor, and thereby that Google, as a processor, acts within the given instructions and does not pursue its own purposes in breach of the data processing agreement.

This impact assessment provides an overview of the investigations and considerations carried out by the local authority in response to the issues raised, and assesses whether, in light of the above, the processing entails a high risk."

However, as stated above, the Danish Data Protection Agency has – as was also the case in the Agency's decision of 14 July 2022 – taken as its basis that Helsingør Municipality does not use Additional Services, but uses only Core Services.

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

Contractual measures

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

The municipality has referred in this regard to the data processing agreement with Google[7], which states the following:

"5.2 Scope of Processing.

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

5.2.2 Google's Compliance with Instructions. Google will comply with the Instructions unless prohibited by European Law. […]" (emphasis added by the Danish Data Protection Agency)

Google's data processing agreement further states the following:

"**2. Definitions**

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

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

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

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

Furthermore, Helsingør Municipality has set out a number of questions to which Google has provided answers. These confirm, amongst other things, that Google processes "Customer Personal Data" solely in accordance with the customer's instructions, and that Google does not process "Customer Personal Data" for its own purposes.

The definition of "Customer Personal Data" covers – as set out in Section 2 of Google's data processing agreement – only information that is entered, stored, sent or received via Google Workspace by the customer or the end user.

It is the Danish Data Protection Agency's assessment that this definition does not cover all personal data that may be generated through the use of Google Chromebooks and Workspace.

In this regard, the Danish Data Protection Agency has placed particular emphasis on Google's own response to the municipality's questions 2 and 3, which states the following:

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

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

- Google processes Customer Personal Data as a processor and only under your instructions. As mentioned in our response to question 1, we do not process Customer Data (including Customer Personal Data) for our own purposes (including advertising purposes), and this commitment is subject to audit by our independent third party auditor.
- **Google processes Service Data as a controller for limited purposes in accordance with our Google Cloud Privacy Notice**. As per our Notice, **Service Data is the personal information we collect or generate during our provision and administration of the Google Workspace services, excluding Customer Data.** We have provided more information about the purposes for which we process Service Data in our response to question 3 below.

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

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

Google may process this Service Data as a controller for the limited purposes described in section "Why we process data" of the Google Cloud Privacy Notice." (Highlighted by the Danish Data Protection Agency)

With regard to the definition of "Service Data", Google's privacy policy (Google Cloud Privacy Notice) of 20 April 2022 states that this includes, amongst other things, the following:

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

- Cloud payments and transactions. We keep reasonable business records of charges, payments, and billing details and issues.
- Cloud settings and configurations. We record your configuration and settings, including resource identifiers and attributes. This includes service and security settings for data and other resources.
- Technical and operational details of your usage of Cloud Services. We collect information about usage, operational status, software errors and crash reports, authentication credentials, quality and performance metrics, and other technical details necessary for us to operate and maintain Cloud Services and related software. This information may include device identifiers, identifiers from cookies or tokens, and IP addresses."

Med hensyn til formålene med Googles behandling af de omhandlede personoplysninger fremgår følgende af privatlivspolitikken:

"Google processes Service Data for the following purposes:

- Provide Cloud Services you request. Service Data is primarily used to deliver the Cloud Services that you and our customers request. This includes a number of processing activities that are necessary to provide the Cloud Services, including processing to bill for services usage, to ensure services are working as intended, to detect and avoid outages or other problems you might experience, and to secure your data and the services you use.
- Make recommendations to optimize use of Cloud Services. We may process Service Data to provide you and our customers with recommendations and tips. These suggestions may include ways to better secure your account or data, options to reduce service charges or improve performance, and information about new or related products and features. We may also evaluate your response to our recommendations.
- Maintain and improve Cloud Services. We evaluate Service Data to help us improve the performance and functionality of Cloud Services. As we optimize Cloud Services for you, this may improve them for our customers and vice versa.
- Provide and improve other services you request. We may use Service Data to deliver and improve other services that you and our customers request, including Google or

third-party services that are enabled via the Cloud Services, administrative consoles, APIs, or the Google Cloud Platform Marketplace or Google Workspace Marketplace.

- Assist you. We use Service Data when needed to provide technical support and professional services as requested by you and our customers, and to assess whether we have met your needs. We also use Service Data to improve our online support, and to communicate with you and our customers. This includes notifications about updates to Cloud Services, and responding to support requests.
- Protect you, our users, the public, and Google. We use Service Data to improve the safety and reliability of our services. This includes detecting, preventing, and responding to fraud, abuse, security risks, and technical issues that could harm our users, our customers, the public, or Google. These activities are an important part of our commitment to secure our services.
- Comply with legal obligations. We may need to process Service Data to comply with our legal obligations, for example, where we're responding to legal process or an enforceable governmental request, or to meet our financial record-keeping obligations.
- Other purposes with your consent. We may ask for your consent to process information for other purposes not covered in this Privacy Notice. You have the right to withdraw your consent at any time.

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

In other words, in the opinion of the Danish Data Protection Agency, the use of Google Chromebooks and Workspace by pupils and teachers generates and collects a range of additional information, which is passed on to Google so that Google may process this personal data for its own purposes, as set out above.

When Helsingør Municipality decides which tools are to be used in the municipality's primary and lower secondary schools, including by individual pupils, it is the municipality that determines the purposes of, and the means for, the processing of personal data that takes place through the use of these tools. Helsingør Municipality is thus the controller for the processing of personal data relating to the pupils and teachers in question, as is also stated in the Danish Data Protection Agency's decision of 14 July 2022.

The decision also states that Helsingør Municipality – as the controller – may not process personal data for purposes other than those provided for in the Primary and Lower Secondary Education Act.

Consequently, the data may not lawfully be disclosed to other controllers for their own purposes where such purposes are not provided for in the Primary and Lower Secondary Education Act. This also includes the processing of personal data that may occur through pupils' use of the equipment and software.

It is the Danish Data Protection Agency's view that the processing of personal data provided for in the provisions of the Danish Primary and Lower Secondary Education Act concerning compulsory education, and which may therefore take place under Article 6(1)(e) of the General Data Protection Regulation, does not include the disclosure of such information 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.

In this case, Helsingør Municipality – as the controller following its decision that the municipality's primary school pupils must use the equipment in question – is disclosing personal data to Google for use for Google's own purposes, as set out in more detail in Google's privacy policy.

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

In this regard, the Danish Data Protection Agency has placed particular emphasis on the fact that Helsingør Municipality's instruction to Google to process only 'Customer Personal Data' for the municipality's purposes does not cover all the personal data processed through the municipality's pupils' use of Google Chromebooks and Workspace, and that there is a range of personal data in the form of 'Service Data' which is collected and disclosed to Google for Google's own purposes.

The Danish Data Protection Agency has also noted that Helsingør Municipality no longer considers it possible to rule out the possibility that Google is acting in breach of its contractual obligations and processing personal data for purposes other than those instructed by the municipality.

Technical measures

Appendix 2 to the documentation sets out the technical measures that Helsingør Municipality has taken to prevent and limit the processing of personal data outside the municipality's instructions. With regard to these measures, it is – following a review thereof – the Danish Data Protection Agency's view that they primarily consist of application settings which prevent or restrict the municipality's pupils and teachers from sharing information with others.

These include, amongst other things, (i) the sharing of documents via dedicated sharing functionality or via shared drives, (ii) restrictions on teachers' access to email attachments, (iii) restrictions on pupils' access to email in general, (iv) restrictions on access to video conferencing, (v) restrictions on access to calendar information, (vi) restrictions on access to Workspace from third countries, etc.

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

These are: (i) disabling the use of personal Google accounts on the Chromebooks in question; (ii) restricting the sharing of diagnostic data with Parallels; (iii) disabling the option to provide Google with user feedback regarding the applications used, (iv) sharing data with Google when clearing the Chrome browser, (v) disabling Google's collection of entered web addresses and metadata for the purpose of improving search and browsing.

It is the Danish Data Protection Agency's assessment that the majority of these settings do not restrict or prevent the generation and collection of Service Data when using Google Chromebooks and Workspace, nor the transfer of such data from Helsingør Municipality to Google.

In reaching this conclusion, the Danish Data Protection Agency has taken into account that the majority of the settings relate to restrictions on the sharing of information by the municipality's teachers and pupils with external parties, and that the remaining individual settings relate solely to selected, specific functionalities within Google Workspace, including, for example, the ability to provide Google with direct user feedback or the collection of entered web addresses.

The Danish Data Protection Agency has also emphasised that the setting restricting the sharing of diagnostic data with Parallels does not prevent the generation and collection of Service Data and its disclosure to Google, as the setting relates to the Parallels application – which, to the Agency's knowledge, is a virtualisation application – and thus not to Google Chromebooks or Workspace.

Against this background, the Danish Data Protection Agency assesses that the technical measures cannot ensure that personal data is processed solely for the purposes of Helsingør Municipality.

Overall, the Danish Data Protection Agency therefore assesses that neither the contractual nor the technical measures are suitable for addressing the risks identified in the documentation submitted.

Furthermore, the Danish Data Protection Agency considers that the identified and described risks do not, in themselves, take sufficient account of all aspects of the processing activity in question.

The Danish Data Protection Agency has emphasised that the identification and description of the risks are based solely on the top layer of the technology stack, namely Google Workspace. By failing to also examine and describe the other elements of Google Chromebooks – such as, amongst other things, the Chrome browser and Google OS – Helsingør Municipality has not identified the full extent of the risks.

Furthermore, it is the Danish Data Protection Agency's view that Helsingør Municipality – by addressing only the aforementioned risks – has failed to include all relevant processing activities that may pose a high risk to the rights and freedoms of data subjects.

As stated above, in its decision of 14 July 2022 – as an indication that the processing activity is likely to present a high risk – assessed in more detail the extent to which information for which Helsingør Municipality is the controller is processed for purposes other than those provided for in the Primary and Lower Secondary Education Act.

Where there is an indication – a likelihood – that a processing activity is likely to present a high inherent risk, a data protection impact assessment must be carried out, cf. Article 35(1) of the Regulation.

It is not sufficient for such an impact assessment to take into account only the individual elements that are likely to entail a high risk. Rather, the purpose of the impact assessment is to describe and assess these – as well as any further – risk scenarios.

It is therefore not sufficient that Helsingør Municipality has only addressed the risks to the rights and freedoms of data subjects in Google Workspace – and not across the entire technology stack, including, amongst other things, the Chrome browser and Google OS.

4.4. Minimum requirements for data protection impact assessments

The provisions of the General Data Protection Regulation (GDPR) on impact assessments and any consultation with the Danish Data Protection Agency are intended to ensure that no processing involving an inherently high risk to the rights and freedoms of data subjects is initiated without the controller having assessed and mitigated **such risks.**

A data protection impact assessment is thus a tool that enables the controller to address the risks that a processing activity may entail in a systematic manner. The minimum requirements for a data protection impact assessment are set out in Article 35(7) of the Regulation and include:

a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and
d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

A comprehensive description of the processing activity, as referred to in Article 35(7)(a), is a prerequisite for the controller to be able to assess and document the lawfulness of the processing activity, as referred to in paragraph 7(b).

Similarly, the factual circumstances relating to the processing activity and its lawfulness are a prerequisite for assessing any risks in the form of deviations from the intended, lawful processing activity, see paragraph 7(c). Finally, this risk assessment, see point (c), is a prerequisite for identifying and taking the relevant and appropriate measures, see point (d).

It is the Danish Data Protection Agency's view that, as part of an impact assessment, the controller must assess the lawfulness of the processing activity before processing commences. This follows from point (b) of the provision and entails an assessment of how all relevant provisions of the General Data Protection Regulation, including in particular Chapters II–V, are complied with when the activity is carried out as intended and designed.

In addition, the controller must assess whether there are any risk scenarios that could result in the unlawful processing of personal data. By such risk scenarios, the Danish Data Protection Agency means potential situations that may arise unintentionally and which involve a deviation from the intended, lawful processing activity.

This could, for example, involve the unintended processing of personal data which the controller is not authorised to process. It could also involve the unintended collection of more information than is necessary in light of the purpose, or the unintended failure to erase data when the controller no longer requires it. Similarly, it may involve unintended transfers to third countries or the use of processors who cannot provide the necessary safeguards to ensure compliance with the General Data Protection Regulation.

It is the Danish Data Protection Agency's experience that carrying out and updating a data protection impact assessment, and the methodology involved, is a useful tool for identifying

any unlawful processing situations. If, whilst carrying out and updating a data protection impact assessment, the controller identifies that the proposed or ongoing processing activity does not comply with data protection rules in one or more respects, the controller must remedy these issues. This can typically be done by amending the contractual basis underpinning the processing activity, if other controllers or processors are involved, or by redesigning the processing activity. In the worst-case scenario, this may mean that the proposed processing activity in question cannot be initiated or, in the case of processing already underway, cannot be continued.

It is therefore a prerequisite for assessing any risks associated with a processing activity that the activity is lawful as intended and designed.

4.5. Helsingør Municipality's 'data protection impact assessment'

Following a review of Helsingør Municipality's documentation dated 1 August 2022, the Danish Data Protection Agency finds that the documentation does not meet the minimum requirements for an impact assessment, cf. Article 35(7)(a)-(d) of the General Data Protection Regulation.

In reaching this conclusion, the Danish Data Protection Agency has taken into account that the documentation does not contain a comprehensive and systematic description of the processing activity, including a technical description of the equipment and applications supporting the processing, cf. paragraph 7(a) of the provision. Instead, the documentation contains only a general description of the types of personal data and categories of data subjects, as well as a general statement of the purpose of the processing activity.

The Danish Data Protection Agency has further emphasised that the documentation contains only a general (i) assessment of the lawfulness of the processing, see Article 5(1)(a) of the Regulation, with regard to the possible disclosure of personal data to Google, (ii) a description of the legal basis for the local authority's processing of personal data, and (iii) a general reference to the fact that the local authority has drawn up policies and procedures to handle the rights of data subjects.

The documentation therefore lacks, amongst other things, a comprehensive assessment of how the processing activity meets the fundamental requirements of Article 5 of the Regulation, which exception under Article 9 of the General Data Protection Regulation forms the basis for the local authority's processing of sensitive personal data[8], and of how the rights of data subjects under Chapter III are specifically observed when using Google Chromebooks and Workspace.

Furthermore, the Danish Data Protection Agency has emphasised that Helsingør Municipality has not identified and assessed all relevant risks associated with the processing activity, that the risks identified by the municipality have not been adequately assessed, as the assessment is based solely on the top layer of the technology stack rather than the entire technology stack, cf. section 4.3. above, and that the municipality has only partially described measures relating to the security of processing, see Article 32 of the Regulation.

It is therefore the Danish Data Protection Agency's overall assessment that Helsingør Municipality – even for those parts of the processing activity which the municipality has described – has not carried out an impact assessment, as required by Article 35(1) of the General Data Protection Regulation, as the documentation dated 1 August 2022 does not meet the minimum requirements set out in Article 35(7) of the Regulation.

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

The Danish Data Protection Agency has been unable to establish that the data protection officer indicated that they had any comments on the documentation prepared.

The Danish Data Protection Agency recommends that Helsingør Municipality include any contributions from the municipality's data protection officer in future impact assessments. The comments from the data protection officer regarding the advice required under Article 35 of the General Data Protection Regulation, (2), are of significant importance in demonstrating that the data protection officer has had the opportunity and scope to carry out the tasks incumbent upon them under Article 39 of the General Data Protection Regulation.

Finally, the Danish Data Protection Agency notes that the controller, pursuant to Article 38(1) of the Regulation, must ensure that the data protection officer is involved sufficiently and in a timely manner, which, in the Danish Data Protection Agency's view, means that the officer – depending on the specific processing activity – should generally be allocated more than one day to review the relevant material.

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

The Danish Data Protection Agency further finds that, by failing to consult the Danish Data Protection Agency in connection with the implementation of what the municipality itself regarded as an impact assessment, Helsingør Municipality has acted in breach of Article 36 of the Regulation.

As set out in section 4.3 above, it is the Danish Data Protection Agency's assessment that the measures taken by Helsingør Municipality with regard to the disclosure of personal data to Google are not suitable for addressing this issue.

In this context, it is the Danish Data Protection Agency's view that Helsingør Municipality, as a statutory body in the – the state school sector – where the processing of personal data can inherently have serious consequences for data subjects, particularly children and young people, as is the case here, and who, under data protection rules, enjoy special protection, must be expected to possess considerable expertise and experience in dealing with data protection issues. This applies not least when the local authority decides to utilise new, complex technology, where the processing of personal data may give rise to a multitude of data protection issues and often entail high risks.

In the Danish Data Protection Agency's view, Helsingør Municipality should have been aware that the contractual and technical measures it had put in place were not suitable for addressing the situation in question, and that any risks had therefore not been reduced to a level lower than high.

With regard to an unacceptable residual risk, the Danish Data Protection Agency refers, amongst other things, to the European Data Protection Board's guidelines on impact assessments, which state the following:

"An example of an unacceptable high residual risk includes instances where the data subjects may encounter significant, or even irreversible, consequences, which they may not overcome (e.g.: an illegitimate access to data leading to a threat on the life of the data subjects, a layoff, a financial jeopardy) and/or when it seems obvious that the risk will occur (e.g.: by not being able to reduce the number of people accessing the data because of its sharing, use or distribution modes, or when a wellknown vulnerability is not patched)."[9]

Furthermore, it is the Danish Data Protection Agency's view that an unacceptably high residual risk may include cases where there may be (i) unauthorised processing, (ii) processing that goes beyond the lawful purposes, or (iii) repeated personal data breaches. This applies in particular where such instances are likely to occur – either due to circumstances arising from a contract relevant to the processing activity, or due to known characteristics of the technology or service used.

Against this background, the Danish Data Protection Agency finds that Helsingør Municipality, in connection with the preparation of its documentation – which, in the municipality's view, constituted a data protection impact assessment – should have consulted the Danish Data Protection Agency, cf. Article 36(1) of the Regulation.

4.7. Relevant topics for impact assessments

For Helsingør Municipality's future work on data protection impact assessments, the Danish Data Protection Agency refers in general to the guidance on impact assessments issued by the Danish Data Protection Agency and the Ministry of Justice, in particular Chapter 4 on 'special cases', as well as the list drawn up by the Danish Data Protection Agency pursuant to Article 35(4) of the General Data Protection Regulation, setting out processing operations that always require an impact assessment to be carried out.

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

"[…] then, it is the responsibility of the data controller to assess the risks to the rights and freedoms of data subjects and to identify the measures29 envisaged to reduce those risks to an acceptable level and to demonstrate compliance with the GDPR (Article 35(7), see III.C.c). An example could be for the storage of personal data on laptop computers the use of appropriate technical and organisational security measures (effective full disk encryption, robust key management, appropriate access control, secured backups, etc.) in addition to existing policies (notice, consent, right of access, right to object, etc.). [...]"

It is the Danish Data Protection Agency's view that a controller – in order to carry out the correct assessment under Article 35 of the General Data Protection Regulation – is obliged to take into account the relevant factors and knowledge relating not only to the processing itself, but also to the solution and technology chosen to support the processing – in this case, Google Chromebooks and Workspace. This includes the entire technology stack used for the processing.

In addition to the directly relevant factual information about the processing activity, including its purpose and proportionality, it will also be relevant to take into account information about the processors used and other types of technology providers. It is particularly relevant to examine:

a) in particular, the information set out in all the terms and conditions contained in the data processing agreement and/or the contract with the technology provider, which specify the terms under which the service is provided,
b) publicly known risk issues or security vulnerabilities in the chosen technology or services, and
c) situations where one's processor and supplier have already acknowledged that there are either unresolved issues or outstanding matters regarding compliance with the General Data Protection Regulation.

Furthermore, it is particularly relevant for the controller, for example, to examine whether the data processing agreement and/or the contract contain terms that make it impossible for the controller to fulfil their obligations under the General Data Protection Regulation. This may, for example, be the case if it is impossible – or extremely difficult – to issue binding instructions to the processor regarding the processing of personal data, or if there are contractual terms which entitle the processor – as an independent controller – to process personal data without the controller having a legal basis for doing so.

Furthermore, it is relevant to investigate whether there have been instances where the technology provider processes personal data for purposes other than the lawful purpose of providing the service (regardless of whether the controller has instructed the provider to do so or not). There may also be cases where the controller does not have the necessary control over the processing of personal data, for example because the contract structure and terms are complicated or even incomprehensible, or because the controller is unable to obtain the necessary overview of how the processor actually handles the personal data.

It may also be relevant to carry out investigations into the technical aspects of the service provision. There may, for example, be cases where – either through the supplier's own information or through publicly available studies – it transpires that, via the service or application provided, the processing of personal data is occurring to a greater extent than is immediately apparent from the contractual basis, and is thus being collected, disclosed or otherwise processed without authorisation.

Finally, it is important to carry out self-assessments and (ongoing) verification, assessment and evaluation of the intended processing activity. This is a requirement in relation to security of processing under Article 32 of the General Data Protection Regulation, but may also, more generally, provide the factors and insights that should prompt the controller to (re)assess whether there are any risks associated with the processing activity in question and, if so, how these can be managed. Another obvious area is the follow-up and evaluation of personal data breaches, as referred to in Article 33 of the Regulation, which the controller experiences.

With regard to relevant methods and considerations for carrying out a data protection impact assessment, particularly when using technology providers, the Danish Data Protection Agency refers to the chapters 'Know your services' and 'Know your provider' in the Danish Data Protection Agency's guidance on cloud computing from March 2022, which is available on the Agency's website; the Agency may also refer generally to ISO/IEC 29 134, which is an internationally recognised standard for conducting impact assessments.

In light of this, it is not clear to the Danish Data Protection Agency how Helsingør Municipality did not, in general and at an earlier stage, assess that the processing activity in question was generally likely to involve an inherently high risk, particularly given that parts of this risk could be mitigated.

In this connection, the Danish Data Protection Agency acknowledges that Helsingør Municipality, as set out in Annex 2 to the documentation, has taken a number of measures which – in the Agency's view as well – limit the risks to the rights and freedoms of data subjects when using Google Chromebooks and Workspace Core Services.

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

The Danish Data Protection Agency refers, inter alia, to Annex 2 to an update of the data protection impact assessment carried out by Amsterdam University of Applied Sciences and the University of Groningen.[12] This contains, amongst other things, further details regarding the personal data collected through the use of Chrome OS and the Chrome browser, irrespective of any settings in Workspace.

The Danish Data Protection Agency also notes that – according to this updated impact assessment[13] – it does not appear possible to mitigate the relevant risk scenarios without changes to the contractual framework underpinning Google's provision of Chromebooks and Workspace, and the technology used for this purpose.

Finally, the Danish Data Protection Agency refers to Google's press release of 17 June 2022 entitled 'New Commitments on the Processing of Service Data for Our Cloud Customers'[14], which states that Google expects to be able to offer the same terms for 'Service Data' as for 'Customer Data', starting in 2023 and in successive phases in 2024. It also states that Google will work on a modification to Chrome OS, which – for so-called "managed systems" – will also include the Chrome browser. These services will, by that time, also be available in a "pure" processor mode.

5. Summary

Following a review and assessment of the material submitted by Helsingør Municipality on 1 August 2022, the Danish Data Protection Agency finds that Helsingør Municipality's processing of personal data through the use of Google Chromebooks and Workspace for Education remains non-compliant with the General Data Protection Regulation, including that the documentation dated 1 August 2022, prepared by Helsingør Municipality, does not comply with Article 35(1) and (7) and Article 36(1) of the General Data Protection Regulation.

The previously issued prohibition of 14 July 2022 is therefore upheld, but amended such that the Danish Data Protection Agency prohibits Helsingør Municipality from processing personal data through the use of Google Chromebooks and Workspace for Education. The prohibition shall apply until Helsingør Municipality has brought the processing activity into compliance with the General Data Protection Regulation as set out in the decision of 14 July 2022 and has complied with Articles 35(1), 35(7) and 36(1) of the Regulation. For processing operations where consultation with the Danish Data Protection Agency is required under Article 36 of the General Data Protection Regulation, the prohibition shall apply until the Agency has issued an opinion pursuant to Article 36(2), or until the Agency authorises the processing at a time prior to the opinion being issued.

A prohibition issued pursuant to Article 58(2)(f) of the General Data Protection Regulation takes effect immediately.

Under section 41(2) (4), a person who fails to comply with a temporary limitation or definitive restriction on processing issued by the Danish Data Protection Agency pursuant to Article 58(2)(f) of the General Data Protection Regulation shall be liable to a fine or imprisonment for up to six months.

The Danish Data Protection Agency further reserves the right to exercise additional powers under Article 58(2) of the General Data Protection Regulation and to impose sanctions under Section 41 of the Data Protection Act, in respect of the circumstances identified in this decision, once definitive evidence has been submitted that fully illustrates the risks posed by the processing operations to the rights of data subjects.

6. Concluding remarks

As a follow-up to the above – though independently of the upheld prohibition – the Danish Data Protection Agency would be very happy to engage in dialogue with Helsingør Municipality regarding the handling of the issue in question. The Danish Data Protection Agency proposes, as a first step, to hold a meeting between the Danish Data Protection Agency, Helsingør Municipality and, if appropriate, Local Government Denmark (KL), and looks forward to receiving a number of suggestions for possible meeting dates.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

[2] Act No. 502 of 23 May 2018 on supplementary provisions to the Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the Data Protection Act).

[3] See DPIA Google G Suite Enterprise, Data Protection Impact Assessment on the processing of personal data on three platforms using the Chrome browser and as installed apps, Version 1 – for consultation with the Dutch Data Protection Authority, 9 July 2020, updated on 12 February 2021, prepared by the Ministry of Justice and Security's Strategic Vendor Management team for Microsoft (DPIA).

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

[5] For further details, see Google Cloud: Data Processing Agreement for G Suite and/or Complementary Product Agreement (Version 2.1) of 19 August 2019, https://workspace.google.com/terms/10293019/dpa_terms.html, Annex A: A18.1.

[6] The European Data Protection Board's guidelines on data protection impact assessments (DPIAs) and determining whether processing is "likely to result in a high risk" under Regulation (EU) 2016/679, p. 12.

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

[8] The Danish Data Protection Agency refers here to Helsingør Municipality's own description of the processing activity, which states that, amongst other things, information on pupil

assessments and well-being surveys is processed. In the Danish Data Protection Agency's view, such information will usually comprise special categories of personal data as defined in Article 9 of the Regulation.

[9] The Article 29 Working Party's guidelines on data protection impact assessments (DPIAs) and determining whether the processing 'is likely to result in a high risk' under Regulation (EU) 2016/679, WP 248, as endorsed by the European Data Protection Board.

[10] Article 29 Working Party Guidelines on data protection impact assessments (DPIAs) and on determining whether processing is "likely to result in a high risk" under Regulation (EU) 2016/679, WP 248, endorsed by the European Data Protection Board.

[11] In recent years, a number of authorities in the Netherlands have carried out data protection impact assessments (DPIAs) on both Google G Suite Enterprise and Google Workspace for Education. These include the assessment prepared by the Ministry of Justice and Security, as well as the assessment prepared for the University of Groningen and Amsterdam University of Applied Sciences, and the update thereto.

[12] Update to the DPIA report on Google Workspace for Education dated 2 August 2021.

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

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