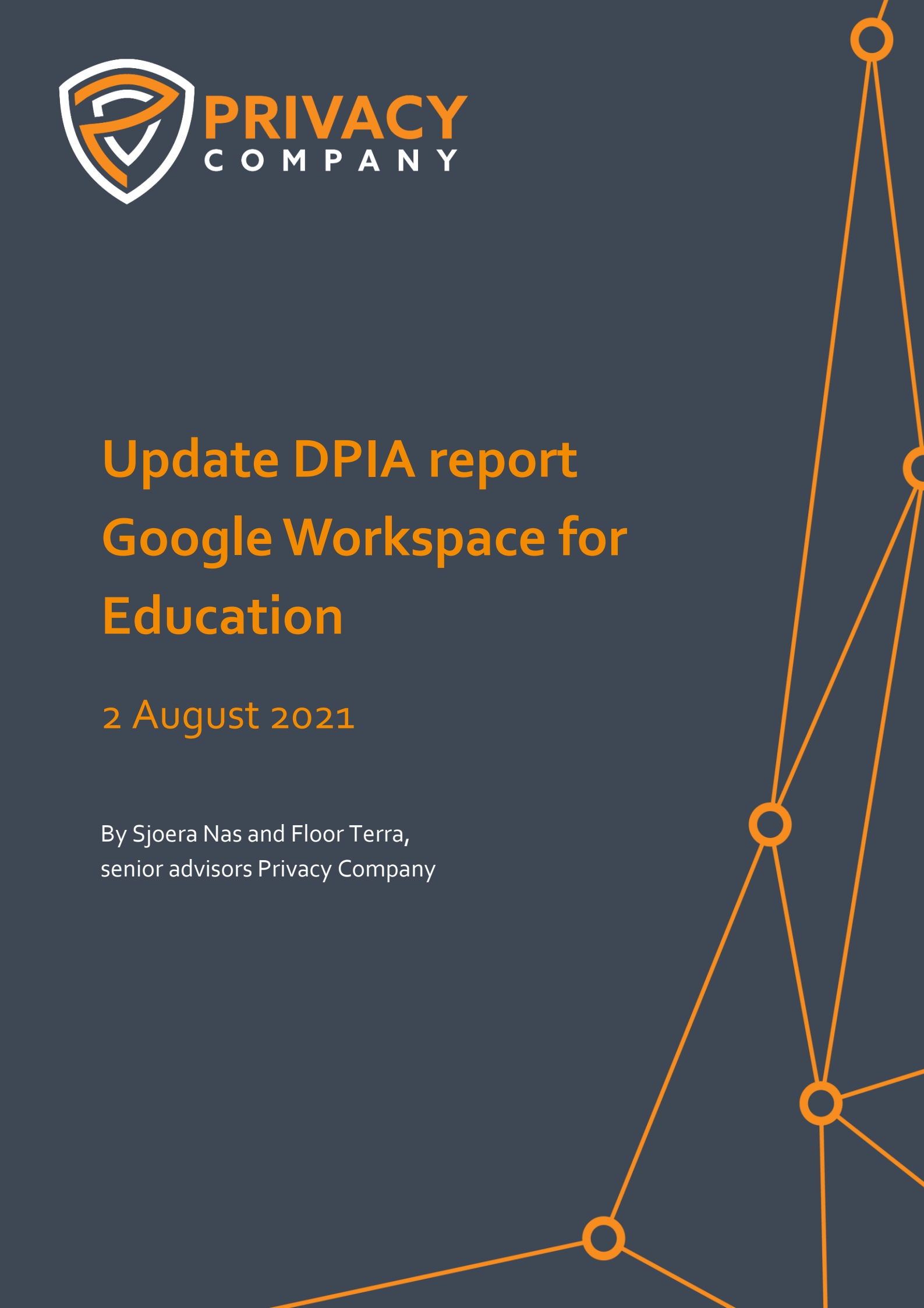
PRIVACY COMPANY

Update DPIA report Google Workspace for Education

2 August 2021

By Sjoera Nas and Floor Terra,
senior advisors Privacy Company



CONTENTS

Summary

This Update DPIA report describes the successful outcomes of the negotiation process with Google to mitigate the high data protection risks resulting from the use of Google Workspace for Education. In the Netherlands 52% of primary schools and 36% of secondary schools use Google Workspace, as well as some faculties at 4 of the 14 universities, and at 4 of the 36 government-funded universities of applied sciences.[1] This can be either the free or the paid (Plus) version.

Thanks to the positive outcome of the negotiations, possible enforcement by the Dutch Data Protection Authority was averted. The Dutch DPA warned the educational sector on 31 May 2021 to stop using Google Workspace if the high risks could not be mitigated before the start of the new school year (21 August 2021).

Results

Google will mitigate the risks through a number of measures. The risks will be mitigated for both the free (Fundamental) and the paid (Standard and Plus) versions of the services. The only two privacy relevant differences between the free and paid version is that paying customers can choose to store content data for certain Core Services in data centres in the EU, and have access to more security features, such as device management.

Google's contractual, organizational and technical measures to lower the 8 high data protection risks are summarised in a table at the end of this Update report. Four highlights are:

1. **Google has agreed to act as data processor for the Diagnostic Data about the individual use of the services.** In a role as data processor Google may only process the personal data for the three (fixed) purposes authorised by the schools and universities, instead of the current 17 dynamic purposes. Google will only process Customer Personal Data and the Google Account Data in the Core Services as data processor, for the three purposes mentioned below, and only when necessary:

    1. to provide, maintain and improve the Services and Technical Support Services subscribed to by Customer;
    2. to identify, address and fix security threats, risks, bugs and other anomalies
    3. to develop, deliver and install updates to the Services subscribed to by Customer (including new functionality related to the Services subscribed to by Customer).

    This improvement lowers three of the high known data protection risks:

    1. loss of control over the Diagnostic Data, because Google's purposes were unspecific and vague, and could be changed anytime,
    2. lack of purpose limitation of the Diagnostic Data, because schools and universities could not instruct Google to only process for purposes they allowed, plus Google

[1] These statistics were collected through questionnaires from SIVON and SURF in July 2021. 1 university and 3 universities of applied sciences answered they expect to completely stop using Google Workspace before the end of 2021. As far as is known, none of the MBOs (equivalent of junior college education) use Google Workspace.

reserved the right to ask pupils and students for consent for unknown new purposes;

3. the lack of a legal ground, because schools cannot obtain valid freely given consent from the (parents of the) children, and prior to the negotiations, legally the schools and universities were joint controllers with Google, but nor Google nor the institutions could base the data processing on a different legal ground from consent.

The full adaptation of the data processor role requires significant technical and organisational changes to Google's systems and processes and can therefore not be implemented overnight. However, the high risks will be mitigated before the start of the new school year.

2. **Until Google releases a processor-version of the Chromebooks with the Chrome browser and a separate processor-version of the Chrome browser** schools and universities can take risk-mitigating technical measures as listed at the end of this blog post. The commitment from Google to create a processor version is an important risk mitigating measure, in particular for primary schools in the Netherlands, as many of them use Chromebooks in school, and many parents have bought Chromebooks at home during the pandemic. As data controller Google permits itself to process the personal data processed on the Chromebook and collected through the browser about the web surfing behaviour from children, students and teachers for 33 broad commercial purposes, including many marketing purposes, behavioural advertising, business development and research.

3. **Google remains a data controller for the services it calls Additional Services such as YouTube, Search, Scholar, Photos and Maps**. As mentioned above, a data controller Google permits itself to process the personal data for 33 broad commercial purposes. Google does protect children and students when they use Search: they are automatically signed-out when they visit Search when they are logged-in with their Google Workspace for Education account. This means Google treats those data as if they were from an anonymous user, and Google cannot use the data for behavioural advertising. Unfortunately, Google does not offer this privacy protective easure for YouTube, Photos, Scholar or Maps. That is why schools and universities must use the option to technically prohibit end users from accessing the Additional Services. Children and students can still use Search after such blocking, but if they want to use other Additional Services, they have to create a separate (private) Google account. Schools can only continue to use YouTube if they embed selected videos in the Core Services, such as Classroom or Slides. Google to confirmed that any cookies in such embedded videos comply with the agreed measures ultimately by the beginning of the new school year.

4. **Google has agreed to become more transparent.** Google will publish significantly more documentation about the different kinds of personal data it collects about the individual use of its services (the Diagnostic Data), develop a data inspection tool for admins to compare the documentation with the data actually stored by Google, make it easier for system administrators to comply with data subject access requests from pupils and students and provide detailed information about the subprocessors for the Diagnostic Data.

The complete list of agreed measures sufficiently mitigates all known high privacy risks identified in the original DPIA, but only if schools and universities also take the following measures: sign up for the contract with the new privacy amendment, implement the recommended (technical and organisational) measures at the end of this Update report, and assess if there are specific additional risks related to their type of school and deployment.

Role of SIVON and SURF

The negotiations were conducted by SURF on behalf of all higher education institutions in the Netherlands, and by SIVON for all primary and secondary education schools in the Netherlands. In parallel, negotiations were conducted by the supplier management office for the Dutch central government (SLM Rijk).

This Update DPIA report should be read in conjunction with the original DPIA on Google Workspace for the Amsterdam University of Applied Sciences (HvA) and the University of Groningen (RUG). The original DPIA was completed in July 2020, updated in March 2021, and published in May 2021.[2]

Advice Dutch data protection authority

After completion of the initial DPIA in July 2020, the Dutch central government and the education sector entered into negotiations with Google. These discussions, held between July and February 2021, only led to the mitigation of 2 of the 10 identified high risks. Because of these remaining high risks, SURF and SIVON requested advice from the Dutch DPA. In its advice of 31 May 2021, the Dutch DPA warned schools and universities and advised the responsible two ministers to stop using Google Workspace before the start of the new schoolyear, if the high data protection risks could not be resolved before that date.[3]

The Dutch DPA advises the schools and the two Ministers to take a number of measures, including assessing the specific risks for children. This group of data subjects was not part of the original DPIA (for the two universities), but as the Dutch DPA notes, careful analysis of the specific risks for children is required, as well as the impact these risks have on children of different ages. This report provides a separate section about the risks for three age groups of children in more detail (ages 6-9, 9-12 and 13-16), and describes how schools and universities can mitigate the remaining risks.

The Dutch DPA emphasises that schools have their own DPIA-obligation. They cannot suffice with a reference to the initial DPIA for the two universities and the analysis in this Update report. Every school and university is responsible, and can be held accountable, to evaluate possible additional risks for the rights and freedoms of the pupils/students and employees, and to determine if the factual use of Workspace for Education is GDPR-compliant.

---

[2] DPIA on the use of Google G Suite (Enterprise) for Education, for the University of Groningen and the Amsterdam University of Applied Sciences, 15 July 2020, update 12 March 2021, URL: https://www.sivon.nl/app/uploads/2021/06/SIVON-Updated-G-Suite-for-Education-DPIA-12-March-2021-v1.2.pdf.

[3] Letter from both ministers of Education to the Lower House, 8 June 2021, with two attachments: the letter sent by the Dutch Data Protection Authority to SURF and SIVON, and the letter sent to Minister Slob of Primary and Secondary Education and Media to guarantee privacy in education with regard to the use of Google G Suite for Education, URL: https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2021Z13300&did=2021D28392

Introduction

On 8 July 2021, the two Dutch Ministers of Education informed the Lower House that agreement was reached with Google on a set of contractual, organizational and technical measures to mitigate the 8 residual high risks identified in the (updated) DPIA on Google Workspace for Education (Plus).[4] Thanks to the positive outcome of the negotiations, possible enforcement by the Dutch Data Protection Authority was averted.

In response to a request for advice from the schools and universities in March 2021, the Dutch Data Protection Authority (Autoriteit Persoonsgegevens) warned schools and advised the responsible two ministers on 31 May 2021 to stop using Google Workspace before the start of the new schoolyear, 21 Augustus 2021, if the problems could not be solved.[5]

The negotiations were conducted on behalf of all the primary and secondary schools in the Netherlands by SIVON, and on behalf of the higher education institutions by SURF. These two cooperatives assist schools and universities with IT procurement. SIVON and SURF consulted the Ministry of Education, Culture and Science and the sector organizations such as the PO-Raad and the VO-Raad during these discussions. In addition to Workspace for Education, the negotiations also addressed the use of Workspace Enterprise by the Dutch central government, represented by Stategisch Leveranciersmanagement (SLM Rijk).

This Update DPIA report describes the mitigating measures in detail, both the measures agreed by Google, and the measures schools and universities should take to ensure GDPR-compliance. The Dutch DPA asked SURF and SIVON to pay specific attention to the risks for children. This group of data subjects was not addressed in detail in the original DPIA as the majority of university students is older than 16. This report provides a separate section about the risks for three age groups of children in more detail (ages 6-9, 9-12 and 13-16), and describes how schools and universities can mitigate the remaining risks.

Background: initial DPIA completed July 2020

The negotiation results are the result of a long process, that started with the completion of the first version of this DPIA on 9 July 2020. This DPIA was performed by Privacy Company for two Dutch universities: for the Amsterdam University of Applied Sciences (HvA) and the University of Groningen (RUG). The DPIA concluded there were 10 high and 3 low data protection risks for data subjects when

[4]Letter from Minister Van Engelshoven of Education, Culture and Science and Minister Slob of Primary and Secondary Education and Media (in Dutch only), Voortgang advies Autoriteit Persoonsgegevens inzake Google G Suite for Education, 8 July 2021, URL: https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2021Z13300&did=2021D28392

[5] Letter from both ministers of Education to the Lower House, 8 June 2021, with two attachments: the letter sent by the Dutch Data Protection Authority to SURF and SIVON, and the letter sent to Minister Slob of Primary and Secondary Education and Media to guarantee privacy in education with regard to the use of Google G Suite for Education, URL: https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2021Z10202&did=2021D22378

universities decided to use G Suite (Enterprise) for Education.[6] Google has since renamed these services in Workspace for Education Fundamentals (the free of charge version) and the paid versions Workspace for Education Standard and Workspace for Education Plus.[7] Because of the lack of transparency and purpose limitation, Google did not qualify as data processor for the processing of any of the personal data it collected in and about the use of its Workspace services. Google and the universities factually operated as joint controllers, and hence could not successfully claim any legal ground for the processing, as required by Article 6 of the GDPR.

Until these high risks were solved, universities were advised not to use Workspace for Education, nor in the free, nor in the paid version.

Interim results March 2021

The universities provided Google with the findings upon completion of the initial DPIA. Between August and January 2020, SURF, SIVON, the central Dutch government and Google discussed measures to mitigate the ten high data protection risks. A major improvement was achieved with regard to purpose limitation for the Customer Data. Google agreed to only process the Customer Data for three authorised purposes, and ensured it would only process the Google Account Data, when used in the Core Services, as processor. Google accepted a prohibition to process Customer Personal Data and/or Diagnostic Data from the Core Services for advertising purposes or for profiling, data analytics and market research.

Google also made improvements to address the lack of transparency, by publishing a detailed admin implementation guide and a separate privacy notice covering Diagnostic Data. Additionally, Google took measures to prevent spill-over of personal data from the educational to the consumer environment. When an end-user accesses an Additional Service such as Google Search or YouTube with a Google Education account, Google ensures that the student is automatically logged-out. Google agreed to an effective audit right to verify compliance with the agreed processing. Last but not least, Google agreed to rephrase the contractual requirement for the schools to obtain consent from the parents of the pupils for the use of the Additional Services to apply only to situations where consent is required and available.

However, these new guarantees and measures only fully mitigated two of the 10 high risks, namely the risks resulting from *the use of one Google account* and from the *privacy unfriendly default settings*. One of the unsolved key problems was the role of Google as a data controller for the Diagnostic, Support and Feedback Data, for the Chrome OS and the Chrome browser and for some frequently used Additional Services such as YouTube, Search and Scholar, while Google did not acknowledge a factual role as joint controller with the schools and universities.

Advice Dutch DPA 31 May 2021

Initially, the negotiations with Google (between July 2020 and February 2021) only led to the mitigation of 2 of the 10 identified high risks. In response to a request for advice from the schools and

[6] See the updated DPIA on the use of Google G Suite (Enterprise) for Education, published in March 2021, published by SURF, URL: https://www.surf.nl/files/2021-06/updated-g-suite-for-education-dpia-12-march-2021.pdf

[7] Google, Choose the edition that's right for your institution, URL: http://edu.google.nl/intl/nl_ALL/products/workspace-for-education/editions/

universities in March 2021, the Dutch DPA warned schools and universities and advised the responsible two ministers on 31 May 2021 to stop using Google Workspace before the start of the new schoolyear, if the problems could not be solved.[8]

The Dutch DPA advises the two Ministers to take the following measures:

- Inform the educational institutions about the advice of the Dutch DPA and the known high risks;
- Investigate how many educational institutions use Google Workspace;
- Inform the educational institutions about the amended privacy conditions;
- Encourage educational institutions to (i) accept the negotiated agreement by SURF and SIVON, (ii) take any additional measures, and (iii) determine whether there are any additional risks compared to the DPIA;
- Provide a list of options for educational institutions to take independent measures to lower the risks;
- Pay specific attention to the risks for children.

The Dutch DPA emphasises that schools have their own DPIA-obligation. They cannot suffice with a reference to the initial DPIA for the two universities and the analysis in the Update report. Every school and university is responsible, and can be held accountable, to evaluate the risks for the rights and freedoms of the pupils/students and employees, and to determine if the factual use is GDPR-compliant.SURF and SIVON will develop tools for the educational institutions to help them comply with this obligation.[9]

The Dutch DPA advises the ministers (in two separate letters):

> *Educational institutions that have not taken adequate measures should make use of the agreements made by SURF and SIVON when deploying Google G Suite for Education, take any additional measures, and determine whether there are any additional risks compared to the DPIA. We also advise the Minister to inform educational institutions of the amended conditions so that they make use of them and are encouraged to carry out risk analyses (or have them carried out).*

This Update DPIA report provides detailed insights in the amended privacy conditions. This report also contains a table with a long list of technical and organisational mitigating measures the schools and universities themselves can take.

---

[8] Letter from both ministers of Education to the Lower House, 8 June 2021, with two attachments: the letter sent by the Dutch Data Protection Authority to SURF and SIVON, and the letter sent to Minister Slob of Primary and Secondary Education and Media to guarantee privacy in education with regard to the use of Google G Suite for Education, URL: https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2021Z13300&did=2021D28392

[9] See www.sivon.nl and www.surf.nl.

The Dutch DPA asked SURF and SIVON to pay specific attention to the risks for children. This group of data subjects was not part of the original DPIA (for the two universities), but as the Dutch DPA notes, careful analysis of the specific risks for children is required, as well as the impact these risks have on children of different ages. This report provides a separate section about the risks for three age groups of children in more detail (ages 6-9, 9-12 and 13-16), and describes how schools and universities can mitigate the remaining risks.

1. Outcome of negotiations 8 July 2021

The negotiations focussed on the following remaining key issues that reflect the remaining 8 high risks identified in the DPIA:

1. Role of Google as data processor
2. Role of Google as data controller for the Additional Services
3. Role of Google as independent data controller for its legitimate business purposes
4. Compliance with the principle of purpose limitation
5. Legal ground of consent with regard to minors
6. Lack of transparency about the Diagnostic Data
7. Retention periods of pseudonymised personal data
8. Use of subprocessors
9. Fundamental right for data subjects to access their personal data.
10. Risks of transfer of personal data outside of the European Economic Area

The results are summarised in ten separate sections below.

One of the key changes, Google's role as data processor for the Diagnostic Data, results in the (partial) lowering of 3 high risks (lack of purpose limitation for the Content and the Diagnostic Data, and the lack of a legal ground as joint controller with the educational institutions). Therefore, this description starts with a precise description of Google's three different roles, as contractually agreed. The agreed purpose limitation (Section 4) has impact on 2 of the high risks (for Content and for Diagnostic Data), while the risks of transfer of personal data outside of the EU were originally classified as a low risk, but have to be assessed by each school and university in a Data Transfer Impact Assessment. This is the result of new legal requirements of the European Commission and new guidance from the data protection authorities in the EU.

1.1. Role of Google as data processor

Google has agreed to become a data processor for the processing of the Account Data and Diagnostic Data in the Workspace Core Services. This solves the high risks identified in the DPIA of the lack of a legal ground when Google and the schools/universities factually act as joint controllers. As explained by the EDPB in its final opinion on the roles of processors and controllers, joint controllership may arise when decisions about the data processing are inextricably linked.[10] Google has committed to only process the Diagnostic Data for the three authorised purposes.

[10] As confirmed by the EDPB in the Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.0, Adopted on 07 July 2021, p.19-20, URL: https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf The EDPB explains: "*As such, an important criterion to identify converging decisions in this context is whether the processing would not be possible without*

Google explained it will take time to systematically redesign and enforce its new role in the capillaries of its complicated data processing architecture. Tthis is technically realistic and acceptable in view of the principled decision to act as data processor. The measures that are put in place before the start of the new school year will mitigate the high risks, meaning that any remaining risks to be mitigated are low risks.

In order to better inform pupils and students when they are interacting with Google as a data processor (in the Workspace for Education services and the Features used from those services, such as Spelling and Maps when used to look-up the location of a calendar appointment), Google will develop an end user profile picture that will be shown on the landing page for all Workspace Core Services (both web and mobile). This will be completed by Q1 2022. The disappearance of the profile picture informs the end users they are leaving the privacy-protected Google Workspace environment.

To prevent any confusion about Google's role as processor for the Account Data when used in the Google Workspace services, Google will make all relevant legal information about the Google Workspace account available in an end user notice by Q1 2022. This will complement the current inadequate sign-up pop-up that contains many hyperlinks and references to Google's consumer privacy policy and terms, and disappears after the student or pupil clicks 'OK'.

Google has also provided SURF, SIVON and the Dutch government with an intention to become a processor for ChromeOS on Chromebooks, and for the Chrome browser, if used on managed devices or with managed profiles. Until Google releases a processor-version of the Chromebooks with the Chrome browser and a separate processor-version of the Chrome browser, admins will have to take mitigating measures. Some of the possible measures are listed in the table at then end of this report, but SURF and SIVON have also commissioned Privacy Company to perform a separate DPIA on the use of Chromebooks in the schools and universities.

1.2. Role of Google as data controller for Additional Services

Google remains a data controller for what it calls *Additional Services*. These services include frequently used services such as Search, YouTube and Google Scholar (see Appendix 1 included in this Update). There are two technical measures to mitigate this risk. First of all, Google automatically 'logs out' pupils and students from their Workspace Education account when they use the search engine. In that case, they are treated as anonymous users and their search data cannot be used for behavioural advertising. However, this is not the case for any other Additional Services, unless they are embedded in the Core Services as feature (such as when Calendar uses Maps to look-up the location of a calendar appointment). Google also applied silent log-out from YouTube for K-12 schools, but will disable this automatic log-out from YouTube per 1 September 2021. From that date,

---

both parties' participation in the purposes and means in the sense that the processing by each party is inseparable, i.e. inextricably linked." See also para 65-67. *"the choice made by an entity to use for its own purposes a tool or other system developed by another entity, allowing the processing of personal data, will likely amount to a joint decision on the means of that processing by those entities."*

end users will no longer be able to access YouTube if the admin has not enabled access the Additional Services. See Section 5 for mitigating measures schools and universities are recommended to take.

When a school has indicated to Google it is a K-12 school, indicating that (some of) the pupils are younger than 18 years, or if a higher educational institution has chosen the K-12 setting, access to the Additional Services is turned off by default. However, if an end user is simultaneously logged in with a consumer Google account and a Google Workspace for Education account, he or she may receive personalised advertising in these Additional Services. Google's default setting for all non K-12 Google accounts is that Ads personalisation is On by default. Google as a data controller refuses to develop a setting for admins to centrally disable this functionality. However, Google has agreed to switch the default setting for Ads personalisation to off for new end users in the Workspace services by Q1 2022. Until then, admins from schools and universities can advise end users to turn this function Off themselves, technically prohibit signing-in with two or more Google accounts, and consider applying the K-12 setting which will reset Ads personalisation to off for all end users (a setting that cannot be overridden by the end users).

1.3. Role of Google as independent data controller

As an independent data controller Google is contractually allowed to process some personal data from the Workspace for Education services for the 7 business purposes, but only when proportionate, such as billing and account management, internal reporting, abuse detection and complying with legal obligations.

This also includes the scanning of content data and check these data against a library of hashed fingerprints for the appearance of known child sexual abuse material (CSAM). If Google detects a match, the end user account is closed. Google then shows a warning to the end-user with an explanation about the reason and available redress mechanisms if the conclusion is incorrect. Google as a data controller may have a legal ground for the processing of special categories of data through the scanning and comparison with fingerprints in Article 9(2) under g and Article 10 of the GDPR, as specified in Article 23, under a and c, of the UAVG (the Dutch implementation law), as the fight against CSAM is an obligation under international law (the UN Convention on the rights of the child, in particular with the Optional Protocol on the sale of children, child prostitution and child pornography[11]).

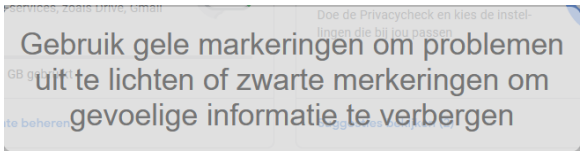
According to a new temporary EU regulation, to enter into effect this summer[12], communication service providers such as Google are permitted, as exception on the confidentiality requirements of

[11] Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, ratified by the Netherlands in 2000, URL: https://www.ohchr.org/en/professionalinterest/pages/opsccrc.aspx

[12] Use of technologies for the processing of data for the purpose of combating online child sexual abuse (temporary derogation from Directive 2002/58/EC), adopted by the EP plenary on 6 July 2021, URL: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0319_EN.html . See for a summary: European Parliament news, Parliament adopts temporary rules to detect child sexual abuse online, 6 July 2021, URL: https://www.europarl.europa.eu/news/en/press-room/20210701IPR07503/parliament-adopts-temporary-

the ePrivacy Directive, to perform this type of scanning on exchanges of documents, e-mails and chats (not audio) to prevent distribution of known or reported CSAM. Any such scanning will also have to apply to the GDPR. However, Google also transfers personal data related to matches to an independent non governmental organisation in the USA, the National Centre for Missing and Exploited Children (NCMEC). Google has explained that Google's US entities are obliged to report hits to NCMEC under US American law. The American mother company, Google LLC, is legally required to apply this scanning to all contents processed globally by any of its subsidiaries such as Google Ireland, not limited to content on its servers in the USA.The possible transfer of personal data to NCMEC leads to a high risk for both senders and recipients. To mitigate this remaining high risk, Google has committed to comply with applicable regulatory guidance, following the advice from the European Data Protection Board (EDPB). The Regulation obliges the European Commission to ask the EDPB within one month after the entry into effect of the Regulation to written advice on the risks of scanning and reporting to the lead DPA for Google, the Irish DPC.

Google also insists on a role as data controller for the support tickets. However, Google has committed to continue to discuss the paradox with SURF and SIVON that Google has agreed to only process both content and metadata as data processor to provide Technical Support Services. Google also acts as processor if a Google support desk employee gains live access to the customer environment, at the request of the customer. Since support tickets may contain personal data, schools and universities are advised not to file support requests via the webform to Google, unless they can ensure such requests do not contain personal data or other sensitive information.



Google also remains a data controller for the content and metadata it may collect when end-users share information with Google in the *Feedback form.* The risk of unlawful processing of personal data

rules-to-detect-child-sexual-abuse-online . The Regulation enters into effect after the formal agreement of the European Council, 3 days after its publication in the European Journal.

is partially mitigated because Google has added a warning to this form to alert end users to the risks of sharing personal or confidential data with Google. To further mitigate this risk, schools and universities are advised to warn staff, pupils and students not to use this form.

1.4. Compliance with the principle of purpose limitation

As agreed in February 2021, as data processor Google may only process the personal data for three authorised purposes, and only when necessary. Google cannot unilaterally change these purposes.

The three authorised purposes are:

1. *to provide, maintain and improve the Services and TSS subscribed to by Customer;*
2. *to identify, address and fix security threats, risks, bugs and other anomalies*
3. *to develop, deliver and install updates to the Services subscribed to by Customer (including new functionality related to the Services subscribed to by Customer).*

This is a vast improvement on the possibilities for the schools and universities to effectively exercise control over the purposes of the processing, compared with the 33 purposes for which Google permits itself to process personal data as a data controller (consumer Privacy Notice), and the 17 purposes for which Google permitted itself to process the Diagnostic Data from Workspace and the Cloud Platform services (Google Cloud Privacy Notice).

This agreed purpose limitation comes on top of the formal prohibition for Google to process any personal data from the Customer Data and the Diagnostic Data from the Core Workspace services for advertising purposes or for profiling, data analytics and market research.

1.5. Legal ground of consent with regard to minors

Google standard terms for Workspace for Education include that Google is a data controller for the Additional Services, and that customer's must obtain consent from the end-users, or in case of minors, consent from their parents. As explained in the DPIA, there is an imbalance of power between parents and schools. Therefore is its highly unlikely that such consent is valid, as parents are frequently not in a position to refuse to provide consent, given that school choices are limited, a majority of primary and secondary schools uses Workspace for Education, and even if a switch to a school that does not use Workspace were a realistic possibility, it would put a huge burden on the shoulders of the pupil. SIVON additionally explained that in practice, it is not possible for schools to obtain consent from all parents in a class.

Google had an elegant solution for schools to prevent having to ask for consent. Google automatically logged out pupils and students from their Workspace account when they visited YouTube, so that their data would be treated as anonymous data, without behavioural advertising. However, Google announced it will terminate this solution on 1 September 2021.[13] After that, if access to Additional Services is not blocked, K-12 end users can only view YouTube content. They won't be able to post videos, comment, live stream, or cast on TVs using a school-managed Google

[13] Google, Control access to Google services by age, URL: https://support.google.com/a/answer/10651918?p=age_based_access_settings

Account. This new set-up still prevents Google from using the viewing data to show personalised ads, but does not prevent showing contextual ads. After 1 September 2021, Google Search will automatically be launched in SafeSearch mode, but there won't be any changes to the silent log-out.

The high risk of processing personal data from minors without legal ground can only be solved if the schools technically disable access from the Workspace for Education accounts to all of Google's Additional Services (currently 54[14], see Appendix 1 included in this Update), to prevent pupils from using YouTube. If pupils still elect to use the full functionality of YouTube on their own initiative, they themselves have to provide valid consent to Google. It is then Google's responsibility as independent data controller to ensure this consent is provided by the parents of the pupil if it is under 16 years in the Netherlands, based on information about the purposes that is easily understandable for children in the different age groups 6-9 years, 9-12 years and 13 to 16 years.

Google confirmed that Google Classroom does not show advertisements in the embedded player. Schools can only continue to use YouTube if they embed selected videos in the Core Services, such as Classroom or Slides. Google to confirmed that any cookies in such embedded videos comply with the agreed measures ultimately by the beginning of the new school year.

1.6. Lack of transparency about the Diagnostic Data

Google has committed to becoming more transparent about the exact personal data it processes as Diagnostic Data, about the different retention periods and their necessity and about processors and third parties that can process personal data from Workspace Education customers. These latter two issues are discussed in two separate sections below.

Google will publish a Help Center article detailing categories and purposes of the processing of diagnostic data (including data collected from cloud servers and telemetry events (atoms) from Android and the Chrome OS by Q1 2022. The level of detail should be sufficiently high for SURF, SIVON and SLM Rijk to verify Google's compliance in an audit. Google will gradually publish information, as it becomes available, over the next six months. Privacy Company has received a confidential list of detailed events Google collects from the Chrome OS, and following discussions about some events that could possibly collect content data, is sufficiently reassured about the contents of these Diagnostic Data. With permission from Google, Appendix 2 to this update contains information about these selected events.

Google will also develop an inspection tool for system administrators to observe the personal data Google stores (and not immediately discards) in its temporary logs, after collecting Diagnostic Data on its cloud servers, and from the end user devices. Google has explained it is not feasible to provide some sort of real time interception tool for the telemetry data (including the atoms from Android), due to the strict security measures and global scale of the data collection.

[14] Google mentions 54 Additional Services. This list does not include the Chrome Browser and the Chrome OS, though they are not part of the Workspace contract. URL: https://support.google.com/a/answer/181865

In combination with the explanations provided by Google about its pseudonymisation processes and retention periods, and the agreed purpose limitation, these commitments are sufficient to mitigate the high risk of the lack of transparency.

1.7. Retention periods of pseudonymised personal data

In the initial DPIA, Google provided limited information about the retention periods of pseudonymised personal data in the Diagnostic Data logs. In June 2021, Google became a bit more transparent, and provided some more explanations about its procedures and policies for the processing of the three different kinds of logs it keeps.

Google retains three different kinds of logs:

1. *Temporary Logs: short term logs with identifiable data which are retained for a maximum of 63 days and then either kept as Archival Logs, or deleted*
2. *Personal Logs: longer term logs which are keyed to internal end-user Id and where end-users have control over retention*
3. *Archival Logs: long term pseudo-anonymous logs and abuse system logs*

Google agreed to publish the following information about is procedures and policies, applying to the collection, the retention and the access controls for the Diagnostic Data, and in particular the guarantees when identifiable data from the temporary logs are transferred to archival logs.

> *Log creation and configuration*
>
> *All logs at Google are defined with an explicit Protocol Buffer schema file. Our policies require schema files to be checked into a specific directory owned and curated by the logging Privacy group. All creation of and modification to schema files are reviewed by this Privacy group, subject to several Privacy by Design principles, including:*
>
> *All fields in the schema are explicitly annotated based on the Privacy-relevant characteristics of the data.*
>
> *These annotations not only cover persistent unique identifiers (including identified and pseudonymous), but these annotations also capture fields from which inferences about identity can be made.*
>
> *Unstructured fields (e.g., key/value pairs or arbitrary strings) are broken down into more granular and explicit fields which can then be clearly annotated.*
>
> *When creating logs, the creation and review process requires engineers to provide several explicit configuration elements including (1) the retention duration of the data, (2) the schema (drawn from the directory above), (3) the declared list of identifier types to be used. The combination of these is reviewed by the logging Privacy group for compliance with retention policies, and to prevent individual logs from containing incompatible identifier types (e.g., pseudonymous together with*

> *identified). The review tooling is designed with technical controls, including flagging of long retention for identifiable data.*
>
> *If the review process identifies a longer retention period (e.g., more than 63 days), one or more cleanup and redaction phases (referred to as Logs Curation), are triggered based on their overall retention schedule. These redaction phases perform activities such as (1) sanitization of personal information (e.g., IP address), and (2) removing cookie IDs, or creating randomized daily session identifiers to replace those cookies.*
>
> *Retention and Post-Processing Controls*
>
> *In addition to privacy review at the log and schema creation stage, we implement additional privacy and security measures later in the data use and storage lifecycle. For example, Logs Validation is an additional technically-supported audit function, which scans sampled data stored in the logs. This data is combined with configuration metadata for the logs to create both alerting based solely on configuration, as well as alerting based on any discrepancies between the logged data and configuration. This Validation includes per-record checks for co-presence of incompatible field types (e.g. identifying and pseudonymous).*
>
> *Logs Access Controls*
>
> *Access to Logs is managed by the same logging Privacy group. Every access request must supply a clear business rationale. To apply for access, employees must affirmatively acknowledge the policies governing use of Logs data. These policies explicitly forbid attempts to reidentify data that has been pseudonymized, and correlation of data between identified and pseudonymized datasets. Analysis of data across multi-day timeframes is covered by specific questions in the access form, since multi-day analysis has a higher chance of reidentifiability.*

In sum, Google takes measures to prevent opaque data collection by requiring the engineers to document every data field. Google scrubs identifiers such as IP addresses and cookie IDs from the logs after some time, performs a check on the possibility to combine identifying and pseudonymous data, takes samples to compare the documentation with the contents of logs, forbids attempts to reidentify pseudonymised data, and generally only permits single day analysis, requiring a higher burden of proof for the necessity for multi-day analysis.

Google has not provided samples or the explicit rules that are checked when assessing the data collection, but has committed to provide a full auditable list of checks and procedures to SURF and SIVON (and the Dutch government) to enable an audit.

These measures help lower the high risks of reidentification of pseudonymous data and unlawful further processing of the Diagnostic Data, as they may be retained in archive logs indefinitely. In view of (i) Google's contractual guarantee that it will only use the term anonymisation in accordance with WP29 guidance, (ii) the negotiated audit right and (iii) the intention of the Dutch government, SURF and SIVON to factually audit Google's compliance with the agreed retention periods, this risk is sufficiently mitigated.

1.8. Use of subprocessors

As part of Google's transition to a role as data processor for all personal data in and about the Google Workspace services, Google has agreed to provide clear documentation about the subprocessors it engages to process the Service Data. Google has assured that it does not use any other subprocessors than currently listed for the Customer Content Data.[15] However, it is currently not clear which subprocessor may process Service Data and for what purposes. Google will provide details about its subprocessors, in particular for the Diagnostic Data, by Q3 2021. Google will specify

- full entity name
- relevant Service(s)
- location(s) where the data are processed
- activity (i.e. what does the subprocessor do)
- whether the subprocessor processes Service Data in temporary, personal and/or archive logs

Once the information is available, SURF, SIVON and the Dutch government will review and assess if the transfer to these parties does not lead to any (new) high risks for data subjects.

1.9. Fundamental right for data subjects to access their personal data

In the original DPIA, Google in its role as data controller categorically refused to provide access to the Diagnostic Data [collected through the Core Workspace Services, the Additional Services, the Features, the Google Account, the Technical Support Services and the Other Related Services such as Feedback and the Enhanced Spellchecker in the Chrome browser].

The DPIA also concluded that Google, in its role as data processor for the Core Services and the audit logs with usage data, failed to provide its education (and Enterprise) customers with sufficient information to adequately respond to data subject access requests.

Now that Google has agreed to become a data processor for all Diagnostic Data, Google has committed to three risk-mitigating measures.

First of all, Google commits to publish in more detail by 21 August 2021 why it generally cannot provide access to Telemetry Data, Website Data and personal data from Google's SIEM security logs, but will consider each request under Article 15 GDPR.

Second, Google will expand the availability of admin audit logs to cover all Core Services and Google will develop a Domain Wide Takeout capability to individual user level/org unit level by 31 December 2022.

Thirdly, Google will provide an inspection tool for admins to inspect the collected telemetry data by 31 December 2022. Google will show SURF and SIVON pilot versions during development.

---

[15] Google Workspace and Cloud Identity Subprocessors, Last updated: 10 June 2021, URL: https://workspace.google.com/terms/subprocessors.html.

The two last measures will greatly increase the possibilities for schools and universities to comply with their obligations as data controllers to respect the fundamental access rights of their pupils and students, and thus lower the high risk for data subjects. Google's improved explanations have to be assessed when they are published. If a student or pupil complains to the Dutch DPA, it is up to the Dutch DPA to assess whether Google's arguments are convincing that it cannot identify the user of cookie data, and in other circumstances, can rely on the exceptions in the GDPR to not provide access.

1.10. Risks of transfer of personal data outside of the EEA

The risk of transfer of personal data outside of the EU was originally classified as a low risk, in July 2020. In the updated version of the DPIA, in March 2021, a reference to Schrems-II and guidance from the EDPB was included, but no in-depth analysis was added of the new situation.

As a result of the jurisprudence in *Schrems-II* of the European Court of Justice and the recently issued finalised guidelines of the EDPB on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data[16], schools and universities have to perform an analysis of the risks of transfers of data outside of the European Economic Area (EEA). This analysis can be called a Data Transfer Impact Assessment.

As outcome of the negotiations, Google commits to providing reasonable assistance and all information required in order to make such an assessment under the Standard Contractual Clauses (SCC). This includes detailed information about the data residency choices offered to Google. These choices can be made with regard to some Core Services, but not to all, and they do not apply to all data.[17] Google commits to providing the types of Customer Data not covered by the data residency policy ultimately by Q3 2021.

This Section 1.10 aims to provide assistance to the schools and universities with their Data Transfer Impact Assessment, based on the new guidance from the EDPB, the new SCCs published by the European Commission and specific information about Google's data protection measures.

Guidance EDPB

The EDPB recommends strong encryption as the best measure to mitigate the risks of unlawful processing when the data are transferred outside of the EEA. High risks can for example result from requests from law enforcement authorities, attacks by (state funded) hackers and unlawful exports by bribed employees. However, the EDPB also acknowledges that end-to-end encryption with customer-held keys is not always possible for cloud providers. For example, if an end user wants to search in Gmail, the contents must be legible for Google. Therefore the EDPB also allows for a risk-

[16] EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2.0, Adopted on 18 June 2021, URL: https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf.

[17] Google, What data is covered by a data region policy, URL: https://support.google.com/a/answer/9223653?visit_id=637617067770477914-2144658213&rd=1

based approach for transfers, assuming all the data, purposes, roles and applicable laws in the country of the importer have been listed in the SCC.

> *"You may decide to proceed with the transfer without being required to implement supplementary measures, if you consider that you have no reason to believe that relevant and problematic legislation will be applied, in practice, to your transferred data and/or importer".*[18]

Exporters must consult a variety of sources. These sources must be "*relevant, objective, reliable, verifiable and publicly available or otherwise accessible*."[19] The EDPB recommends reading the transparency reports from the importing organisation. However, "*Documented practical experience of the importer with relevant prior instances of requests*" alone cannot be relied on.[20] Annex 3 of the EDPB guidelines contains a non-exhaustive list of sources to consult, such as reports from various credible organisations and (disappearance of) warrant canaries from other entities.

Google's policy and transparency reports

Google's policy with regard to disclosures to law enforcement is extensively described in the original Google Workspace DPIA for the RUG and HvA, and is not repeated here. This update about Google's guarantees is limited to information about new statistics from Google in transparency reports, news about a refusal from Google to disclose personal data, and general news about the increasing amount of law enforcement requests and gagging orders in the USA.

Between July 2019 and December 2019, Google received one law enforcement request for disclosure of Dutch Workspace Enterprise customer information. Between January 2020 and July 2020, Google received zero requests for disclosure of Dutch Workspace Enterprise customer information. In total, in the first half of 2020, Google received 398 requests for disclosure of Google Workspace Enterprise customer information, relating to 478 cloud customers. Google honoured 39% of the requests.[21]

Google has a strong track record of resisting unlawful government requests. Most recently, Google refused a request from the US Justice Dept to hand-over Diagnostic Data from emails of New York Times reporters. The New York Times reports:

> *"Google fought a gag order this year on a subpoena to turn over data on the emails of four New York Times reporters. Google argued that its contract as The Times's corporate email provider required it to inform the newspaper of any government requests for its emails, said Ted Boutrous, an outside lawyer for The Times."*[22]

---

[18] EDPB, Recommendations 01/2020, Version 2.0, para 43.3.

[19] Idem, para 46.

[20] Idem, para 47.

[21] Google, Enterprise cloud requests for customer information, URL: https://transparencyreport.google.com/user-data/enterprise?enterprise_user_requests_report_period=product:2;authority:;time:;series:requests,accounts&lu=enterprise_user_requests_report_period&hl=en_GB

[22] New York Times, 11 June 2021, In Leak Investigation, Tech Giants Are Caught Between Courts and Customers, URL: https://www.nytimes.com/2021/06/11/technology/apple-google-leak-investigation-data-requests.html

Increasing amount of gagging orders in the USA

The New York Times also reveals that

> *"the number of these requests has soared in recent years to thousands a week, putting Apple and other tech giants like Google and Microsoft in an uncomfortable position between law enforcement, the courts and the customers whose privacy they have promised to protect."*

Microsoft President Brad Smith revealed in an Opinion in the Washington Post that *prosecutors too often are exploiting technology to abuse our fundamental freedoms.* He also warned against the default use of gagging orders.

> *"Not long ago, if the government wanted to serve a search warrant as part of a criminal investigation, it had to do so in person, with notice. An agent or officer needed to bring a signed warrant to a house or building and hand it to the target of the probe at the front door; only then could the government search the premises for documents, records and computer files. This was true for individuals, businesses and governments alike. If secrecy required getting a "sneak and peek" warrant because evidence would be destroyed in advance or a witness's safety would be jeopardized, this required a heightened showing, beyond mere probable cause.*
>
> *Those principles still hold true today. Yet with the expansion of cloud computing in every industry, the federal and state governments know they quickly can obtain data electronically from sources other than the target. So that's what they do. In secret. By serving search warrants on companies such as Apple, Google and Microsoft to obtain emails and messages that belong to our customers. Government prosecutors also ask courts to impose gag orders on companies such as ours that prevent us from letting people know that copies of their emails are now in the government's hands."*[23]

This news about the high amount of secrecy orders in the USA makes it difficult to rely on Google's transparency statistics, as Google may be prohibited from disclosing the real amount of disclosures.

New SCCs from the European Commission

In the new SCC published on 4 June 2021[24], the European Commission unexpectedly changed the definition of international transfers. Apparently, it is no longer the case that every transfer of personal data to a system outside the EU/EEA is qualified as an international transfer. Rather, a transfer only qualifies as an international transfer if the personal data will no longer be directly protected by the GDPR in the recipient (third) country. The new SCC include a sentence in a recital explaining that

[23] Washington Post, Opinion Brad Smith, The secret gag orders must stop, 13 June 2021, URL: https://www.washingtonpost.com/opinions/2021/06/13/microsoft-brad-smith-trump-justice-department-gag-orders/

[24] European Commission, Standard contractual clauses for international transfers, URL: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en

organisations cannot use the SCCs if the GDPR already applies to the importer in the third country anyway.[25]

The unexpected move by the Commission has created uncertainty about how the new SCCs should be used. If the Commission's interpretation stands, and transfers will from now on only qualify as international transfers if the GDPR is not already applicable to the importer, it is unclear how organisations can prevent laws in the receiving country undermining the GDPR, and act in accordance with the ruling of the Court.

Google has a GDPR-relevant establishment in Ireland. This means Google is already subjected to the GDPR following the territorial scope of the GDPR determined in Art. 3(1). This means it is unclear if the schools and universities can use the new SCC's for transfers. The final version of the recommendations from the EDPB about technical measures for international transfers (quoted above) does not shed light on the DPAs views on the new definition. The document does however contain some suggestions about the DPAs' position.

For example, the DPAs write that the fact that a person outside the EU/EEA can access data stored in the EU already constitutes an international transfer. They also state that if a data controller in the EU uses an international cloud provider, this constitutes an international transfer. Only when a controller is certain that its cloud provider has an office located the EU and that the data remains within the EU, the DPAs find there is no international transfer. A contrario, this sentence can be read that the DPAs find there is international transfer if the cloud provider has an office located in the EU, but the data do leave the territory of the EU. This is remarkable, as the presence of an establishment in the EU specifically indicates that the cloud provider must already comply with the provisions of the GDPR, and the export of the data to a territory outside of the EU should not matter. According to the Commission's interpretation, there should be no objection to using the data in the importing country if the is GDPR still applicable. Apparently, the EDPB disagrees.

Unfortunately, it will take some time before there will be more clarity. The new explanation of the Commission about the non-applicability of Chapter V of the GDPR goes against all previous interpretations of data protection authorities (DPAs) and the European Court of Justice. After all, the Court ruled that a transfer of data from Facebook Ireland to Facebook Inc. in America constitutes an international transfer of data, while the GDPR clearly applies to Facebook, Inc, because of its lead establishment in Ireland and also because of the offering of goods and services to people in the Union.

Privacy experts Douwe Korff and Ian Brown draw the conclusion that international transfer does happen (Chapter 5 of the GDPR applies) if the data can be accessed by law enforcement authorities. In a research paper for the European Parliament about the consequences of the Schrems-II ruling for transfers of personal data to the USA they write:

> *Recently the Commission has suggested in two different contexts that SCCs need not, and indeed cannot, be used for transfers of personal data to a data importer in a non-adequate third country, if the data importer in that non-adequate third*

[25] SCCs for international transfers, recital 7: "The standard contractual clauses may be used for such transfers only to the extent that the processing by the importer does not fall within the scope of Regulation (EU) 2016/679."

> *country is itself subject to the GDPR, because the processing relates to the offering of goods or services to data subjects in the Union or the monitoring of their behaviour as far as it takes place within the Union (cf. Article 3(2)GDPR).There is some sense in this: the whole point about SCCs is that they seek to impose on the data importer, by contract, the relevant GDPR obligations that apply if the processing took place in the EU, and it does not make much sense try and impose such obligations in this way if they already rest on the importer by virtue of the law (the GDPR) itself.*
>
> *However, that does not mean that transfers of personal data to an importer in a non-adequate third country who is de iure subject to the GDPR (by virtue of Article 3(2)) can take place without the need for (supplementary) safeguards. The same reasoning as was applied by the Court to transfers to the USA under SCCs also applies here: the mere fact that the EU says the importer is subject to the GDPR does not mean that the data will not be subject to undue access by the authorities of the third country.*[26]

Because Google cannot legally prevent such undue access by authorities in the USA, it would be better to continue working with both criteria for transfer: both when the data leaves the Union (Chapter V) and when sharing data with a party to whom the GDPR does not apply (Article 3).

Based on the current circumstances, schools and universities are advised to accept Google's new SCCs, to at least document the applicable data, purposes, and relevant risks in the importer country. The Data Protection Officers of the schools and universities may contact the special helpdesk of the Dutch DPA to ask for advice if they are not sure if it is legitimate to accept the new SCCs as means to legitimise the transfer of limited personal data to Google's servers in the USA, as these personal data can possibly be accessed by law enforcement authorities in the USA.

Additionally, schools and universities can consider using the newly announced Workspace encryption features for sensitive and confidential data (launched after the negotiations with Google, details not yet published and effectivity not yet analysed).[27]

SURF and SIVON will update the educational institutions about new developments or insights in the transfer of personal data outside of the EEA.

---

[26] Exchanges of personal data after the Schrems II Judgment, Study requested by the LIBE committee of the European Parliament, PE 694.678– July 2021, p. 59, URL: https://source.chromium.org/chromium/chromium/src/+/main:google_apis/gcm/protocol/checkin.proto https://www.europarl.europa.eu/RegData/etudes/STUD/2021/694678/IPOL_STU(2021)694678_EN.pdf

[27] Google, Google Workspace delivers new levels of trusted collaboration for a hybrid work world, 14 June 2021, URL: https://cloud.google.com/blog/products/workspace/new-google-workspace-security-features .

Full list of mitigating measures by Google

No.	Risk	Mitigating measure Google
1	**Lack of purpose limitation Customer Data**	Google will only process Customer Personal Data and Account Data as data processor, for three purposes, when necessary: 1. *to provide, maintain and improve the Services and Technical Support Services (TSS) subscribed to by Customer;* 2. *to identify, address and fix security threats, risks, bugs and other anomalies* 3. *to develop, deliver and install updates to the Services subscribed to by Customer (including new functionality related to the Services subscribed to by Customer).*
		Google will not process Customer Personal Data and/or Service Data for Advertising purposes or for profiling, data analytics and market research.
		7 purposes identified for which Google may process Customer Data as independent data controller. 1. billing and account management and customer relationship management and related correspondence with Customers and Customer Administrators; 2. improving and optimizing the performance and core functionality of accessibility, privacy, security and IT infrastructure efficiency of the Cloud Services and TSS; 3. internal reporting, financial reporting, revenue planning, capacity planning and forecast modeling (including product strategy); 4. abuse detection, prevention and protection (such as automatic scanning for matches with identifiers of CSAM, virus scanning and scanning to detect AUP violations); 5. processing of Personal Data in support tickets and support requests ((including corresponding with Customers and Customer Administrators) and any attachments thereto) sent by Administrators to Google; 6. receiving and using Feedback; and 7. complying with legal obligations. For clarity, the rendering of TSS is a processor activity. With regard to content scanning for Child Sexual Abuse Material (CSAM) and reporting 'hits' to NCMEC, Google will comply with applicable regulatory guidance from the EDPB.
		Google assures that machine learning to improve the contents of Spelling and Grammar Data is limited to within the customer's own Enterprise domain.
		Definition of anonymisation included in the privacy amendment, in accordance with WP29 guidance on anonymisation techniques.
		The framework contract specifies how Google deals with *gagging orders* when ordered to disclose Content Data to law enforcement authorities.
2	**Lack of purpose limitation Diagnostic Data**	Google will only process Diagnostic Data as data processor by the start of the new school year, for the three purposes mentioned above, when necessary. Google will ensure that the 17 purposes in the Google Cloud Privacy Notice will not apply to the use of Workspace by Dutch schools and universities.
		Google will not process Customer Personal Data and/or Service Data for Advertising purposes or for profiling, data analytics and market research.
		Google will switch the default setting for Ads Personalization to Off for new end users by Q1 2022 (relevant for the use of Additional Services). In the K-12 Workspace for Education version this is already off by default. When schools and universities switch to the K12 setting, Ads Personalization will automatically be switched Off. K-12 end users cannot override this Ads Personalization setting
		Google will provide Dutch education institutions with a separate 'data processor' version of the Chrome OS and the Chrome browser on Chromebooks, and a separate data processor version of the Chrome browser for managed devices/managed profiles

		The framework contract specifies how Google deals with *gagging orders* when ordered to disclose Diagnostic Data to law enforcement authorities.
3	**Lack of transparency Customer Data**	Google will develop an inspection tool to provide access for admins to contents of Customer Data in Diagnostic Data (including telemetry data and use of Features), if stored and not immediately scrubbed, by 31 December 2022.
		Google provides a new warning to end users in the Feedback form not to share sensitive data with Google
		Google will show an end user profile picture on the landing page for all Workspace Core Services (both web and mobile) by Q1 2022.This picture will disappear when end user leaves the privacy protected Workspace services.
		Google will make all relevant legal information about the Google Workspace account permanently available in an end user notice by Q1 2022.
		Google has improved its explanation to admins in the Data Protection Implementation Guide that Google processes Account Data as a processor when the Google Account is used in the Core Services.
		Google has not announced measures to provide exhaustive and comprehensible information and visually clarify the difference between the three different spellingcheckers
4	**Lack of transparency Diagnostic Data**	Google will publish a Help Center article detailing categories and purposes of the processing of diagnostic data (including data collected from cloud servers and telemetry events (atoms) from Android and the Chrome OS by Q1 2022.
		Google will expand the availability of admin audit logs to cover all Core Services and Google will develop a Domain Wide Takeout capability to individual user level/org unit level by 31 December 2022.
		Google will provide an inspection tool for admins to inspect the collected telemetry data and data generated on Google's cloud servers by 31 December 2022. Google will show pilot versions to SIVON and SURF during development.
		Google confirmed that all subprocessors that process Diagnostic Data also process Customer Data, and are therefore already included in the list of subprocessors for Customer Data. Google will publish the necessary details per subprocessor about the categories of data, purposes and locations by Q3 2021.
		Google will make all relevant legal information about the Google Workspace account permanently available in an end user notice by Q1 2022.
5	**No legal ground for Google and schools/universities**	Google asks pupils and students for consent for the data processing in the Additional Services (in its role as data controller). It is Google's responsibility to obtain valid consent, not the schools' and universities'.
		Google becomes a data processor for the Diagnostic Data, but not for the support tickets with attachments and Feedback Data.Schools and universities are advised not to use these services, to prevent becoming joint controllers.
		With regard to the (separate) legal ground for the reading of cookie and telemetry data from end-user devices, as defined in the ePrivacy Directive, Google will follow regulatory guidance.
6	**Missing privacy controls**	Google enables admins to take 4 of the 6 measures recommended in the initial DPIA report: • Google will not re-use of content from *Spelling and Grammar* for machine learning outside of the Enterprise customer's domain • Admins can prohibit the use of Additional Services when logged in with an Education account • Admins can apply policy rules to disable the Enhanced Spellchecker in the Chrome browser, without the separate Chrome Education Upgrade. • Google will change the default setting for new users for Ads Personalization to Off by 31 December 2022 (in Education versions for primary and secondary schools (K-12 schools) it is already off by default).

		Additionally, Google will publish detailed information about the telemetry events it collects from Workspace, incl. for Android, by Q1 2022.
7	**Lack of control third parties / processors**	Google will provide details about its subprocessors, in particular for the Diagnostic Data, by Q3 2021. Google will specify o full entity name, o relevant Service(s), o location(s) where the data are processed, o activity (i.e. what does the subprocessor do, o whether the subprocessor processes Service Data in temporary, personal and/or archive logs.
8	**No access for data subjects**	Google will publish details by the start of the new school year why it generally cannot provide access to Telemetry Data, Website Data and personal data from Google's SIEM security logs. Google has confirmed it will consider each request under Article 15 GDPR (i.e. no rejection by default)..
		Google will expand the availability of admin audit logs to cover all Core Services and Google will develop a Domain Wide Takeout capability to individual user level/org unit level by 31 December 2022.
		Google will provide an inspection tool for admins to inspect the collected telemetry data and data generated on Google's cloud servers by 31 December 2022. Google will show SURF and SIVON pilot versions during development.
9	**Transfer of personal data to the USA**	Google will offer the new SCCs for transfers outside of the EEA.
		Google will provide reasonable assistance and all information required in order to make a Data Transfer Risk assessment under the SCC in Q3 2021.
		Google will provide detailed information in what Core Services customers can choose to store the Content Data in the EU, and in what Core Services such a choice is not available by Q3 2021.

Checklist mitigating measures by schools and universities

In principle, the measures listed below should be taken by system administrators of both schools and universities. The term 'schools' includes schools in primary and secondary education in the Netherlands, including special schools. Google uses the US American term K-12, with which Google defines schools with pupils under 18. When the recommended measures differ, for example because Google uses some more privacy friendly settings in the K-12 version of Workspace for Education, the responsibility is allocated by underlining the word 'schools' or 'universities'.

General requirements

- ☐ Accept the new privacy amendment in the contract with Google (through a supplier).
- ☐ All customers of Google Workspace for Education should determine if they wish to self-qualify as K-12, and benefit from with the more privacy friendly defaults, or use the standard offering for Workspace for Education.
- ☐ Schools and universities must conduct their own DPIA on the use of Google Workspace services, Chromebooks and the Chrome browser, based on the original DPIA and the Update DPIA for SIVON and SURF.

Purpose limitation

- ☐ Schools should not enable access to Additional Services (disabled by default in K-12) and on managed devices/managed profiles block the simultaneous use of consumer Google accounts in the Workspace environment. This prevents the risk of spill-over of personal Content Data from the school to the consumer environment (and vice versa). When access is blocked, pupils can still use Search with automatic log-out (in SafeSearch mode).
- ☐ Instruct teachers how to embed YouTube videos in the Core Workspace Services Classroom and Slides rather than using YouTube directly.
- ☐ Universities must disable access to Additional Services, turn off access to new Additional Services when they appear and on managed devices/managed profiles block the simultaneous use of consumer Google accounts in the Workspace environment. Students can continue to use Search when Additional Services are blocked, as this results in automatic log-out. However, if students elect to use Scholar, YouTube or other Additional Services, they have to sign-up individually with Google for a consumer account. Google, and not the universities, is responsible for obtaining valid consent from students for the data processing in such private Google accounts
- ☐ Universities must change the default setting of the Marketplace to prevent access by default by third parties to Customer Data. Pupils from K-12 schools cannot install any apps by default.

- Universities should encourage students to use incognito mode when using Scolar, to prevent joint responsibility with Google for data processing in the Additional Services and data spillage from the educational to the private consumer environment.
- Universities should advise students and teachers to turn Off Ads personalisation in the Google Account themselves when they use Additional Services (turned off by default in K-12). Consider choosing the K-12 setting to switch Off Ads Personalization for all existing and future end users.
- Warn admins not to use Google Support Services until Google becomes a data processor for the support tickets and attachments. Or (create a policy to) only send anonymised requests.
- Warn pupils, students and teachers not to use the Feedback forms, or not to include sensitive information and personal data in Feedback forms (to compensate for the lack of a central privacy control).

Transparency

- Schools must inform pupils and parents that they technically block the use of private Google accounts on school managed devices and profiles, but cannot prevent the use of private Google accounts on private mobile phones. Google, and not the schools, is responsible for obtaining valid consent from children for the data processing in such private Google accounts.
- Provide high level information to pupils and students about the data processing by Google in Workspace for Education, in particular the privacy risks resulting from the use of Additional Services.
- Provide end users with information about the spellcheckers included in the Data Protection Implementation Guide.
- Inform end users that if the profile picture disappears, this means that they have left the privacy protected Workspace for Education environment.
- Read the Google Workspace for Education Data Protection Implementation Guide.[28]
- Use the future data inspection tool to compare the documentation in Google's promised new Help Center Article with the data obtained via this tool. Assess if risks in the DPIA need an update based on the results of the inspection of Diagnostic Data.
- SURF and SIVON can assess the accuracy of the documentation in an audit together with SLM Rijk.
- Access the new audit logs and use the domain wide takeout in response to data subject access requests when available.

[28] Google Workspace Data Protection Implementation Guide, URL: https://services.google.com/fh/files/misc/google_workspace_edu_data_protection_implementation_guide.pdf

- If a student or pupil complains that the reply to a data subject access request is incomplete, it is up to the Dutch Data Protection Authority to assess whether Google's arguments are convincing that it cannot identify the user of cookie data, and in other circumstances, can rely on the exceptions in the GDPR to not provide access.

Chromebooks and Chrome browser

- Until the processor version is available [and has been tested], consider using another default browser (on devices not using ChromeOS).
- Apply the mitigating measures in the future DPIA on Chromebooks for Education by Privacy Company for SIVON (Fall of 2021). In the meantime, consider using the following central privacy enhancing options in the Google and Chrome Admin console:
    - Disable Google Search as default search provider
    - Disable Diagnostic Data sharing with Google to improve the Chrome OS
    - Disable sharing of Diagnostic Data from apps and websites with Google to suggest new content
    - Require verified access
    - Centrally select the standard security level for Chromebooks (do not allow end-end users to enable enhanced safe browsing)
    - Prohibit synchronisation of data with the Google account in the Chrome browser (Chrome Sync)
    - Disable data sharing with Google in the Chrome browser to Make searches and browsing better (uploads all visited URLs)
    - Disable data sharing with Google in the Chrome browser through autofill of searches and URLs
    - Disable data sharing with Google to improve features and performance of the Chrome browser
    - Disable data sharing with Google in the Chrome browser through the Enhanced Spellchecker (centrally prohibit users from turning this feature on)
    - Block third party cookies and trackers in the Chrome browser and consider the use of an adblocker

Control over subprocessors

- Once available, SURF and SIVON will assess the additional information about the subprocessors and may provide educational institutions with guidelines or recommendations based on the outcome of this review. Education institutions should monitor and follow this guidance.

Risks with regard to data transfer to the USA

- Accept Google's new transfer SCCs once available. Conduct a Data Transfer Impact Assessment with the help of input from this Update report. Data Protection Officers of the schools and universities may contact the special helpdesk of the Dutch DPA to ask for advice about the use of the new transfer SCCs, if they are unsure if they can accept them, since the GDPR may already apply to Google as importer.
- Choose data storage in the EU where possible – consider to change to Workspace for Education Plus.

- Consider using the newly announced Workspace encryption features for sensitive and confidential data in relation to possible high risks, once available.
- Warn pupils, students and teachers not to use directly identifying or confidential names in file and pathnames of files they work on in Google Workspace, to lower possible high risks of data transfer to the USA.

Specific risks and measures for children

In its letter to the Minister responsible for primary and secondary education, the Dutch DPA emphasises that schools must conduct a specific risk analysis with regard to children. The Dutch DPA also recommends that SURF and SIVON actively inform educational institutions about their responsibilities in determining the risks for children when they use digital tools, and provide resources to encourage educational institutions to carry out or commission such a risk analysis.

The Dutch DPA writes [translated by Privacy Company]:

> *This requires a careful analysis of the specific risks for children and the impact these risks have on children of different ages. In this respect, it is insufficient to position children as data subjects with a lower age, as children are less aware of the risks and consequences involved in the processing of their personal data. In addition, risks may have a different impact and effect on children than on adults. The systematic recording of data on children's behaviour and development can lead to risks such as discrimination and exclusion.*

Classification in different age groups

In relation to the use of ICT, the risks for children may differ according to their age. This analysis uses three different age groups: 6-9, 9-12 and 12-16 years. This classification was made by SIVON and has been checked with expert Remco Pijpers, strategic advisor digital literacy + ethics of Kennisnet.

6-9 years old

In this age group, children learn to read and write, and start to use ICT. Younger children (4-6) may already encounter the Google ecosystem, when the teacher shows YouTube clips on the whiteboard in the classroom. Both at home and at school children watch lots of YouTube clips, even at a very young age.[29] However, under 6 it is less likely that the school will create individual Workspace accounts.

9 - 12 years

This age group is defined as a separate category, because at this age, children themselves start to use mobile phones. They share their lives and worlds with each other and with the outside world without being aware of the dangers/risks.

12-16 years

At age 12 children enter secondary education schools. The use of ICT is normal. They generally have their own mobile smartphones, and link their school accounts to their private accounts.

[29] As evidenced by the annual Iene Miene Media study 2021, URL: https://www.mediawijzer.net/?smd_process_download=1&download_id=97949

Categories of data provided through Google Workspace

If schools create Google Workspace accounts for children under 16, on average, based on questionnaire from SIVON, they provide the following kinds of personal data to Google:

- Last Name
- First name
- E-mail address
- Name of school (in the email address)
- Date of birth (occurs)

It follows from the questionnaire that teachers and school administrators additionally (incorrectly) store some of the data from their pupil administration system (leerlingadministratiesysteem) or pupil monitoring system (leerlingvolgsysteem) in Google Workspace services.

This concerns:

- Result data (study path, including learning materials) (occurs)
- Educational monitoring data (pupil coaching) (occurs)
- Class, group year, type of education
- Pictures/videos of the pupil (according to the schools, only with consent from the parents)

General risk mitigating measures Google

Google enables schools to self-select the K-12 setting in Workspace for Education. With K-12, Google Google refers to US grades 1 – 12 (i.e. all children under 18). Google does not check the self-qualification of a school.[30] Google applies specific privacy protective measures in the K-12 version of Google Workspace for Education.

- Ads personalisation is turned Off by default and cannot be switched On by end users;
- Access to Additional Services is turned Off by default and cannot be switched On by end users;
- Access to the Marketplace and Google Play is turned Off by default[31] and cannot be switched On by end users;
- Per 1 September 2021, Google will make some changes to the use of Additional Services such as YouTube, Search, Google Play, Maps, Earth and Photos, if schools would enable their pupils to access these services.[32]

[30] Google, Select your organization type for Google Workspace for Education, URL: https://support.google.com/a/answer/7332340?hl=en&ref_topic=3035696

[31] Google for Education Help, Turn on additional Google services, URL: https://support.google.com/edu/setup/answer/6273503?hl=en&ref_topic=6206654

[32] Google, Control access to Google services by age, URL: https://support.google.com/a/answer/10651918?p=age_based_access_settings

Risks 6-9 years

At this age, children may start to independently use applications such as YouTube (Kids[33]) and the Chrome browser. Google is a data controller for these two services. Though Google promises not to use information about the viewing and surfing behaviour for behavioural advertising by kids with K-12 Workspace accounts, Google may still use the personal data about the viewing and surfing behaviour of the children for all other purposes from its general privacy statement. This includes the use of personal data for different marketing and undefined research purposes.

Mitigating measures 6-9 years

Schools should first consider the necessity of creating individual Google Workspace accounts for these children. If they provide a Google account, end users should not enable access to the Additional Services, and only use YouTube clips as embedded material in the Google Classroom (a Core Workspace for Education Service). Schools should not publish audio-visual material from events organised by school with identifiable children on YouTube. Viewing clips on YouTube generally also results in the reading of tracking cookies. Schools may consider using another default browser on school computers, with privacy friendly settings, as long as Google does not offer a processor version of Chrome.

Even if schools choose storage in the EU for Customer Data in Google Drive, they are advised not to store any special categories of data relating to the children without additional measures, such as encryption. This applies in particular to the Diagnostic Data, that are processed in the USA. They should not upload any individual result data or educational monitoring data, or information about the class, group year and type of education of the pupils to Google Workspace services, not attached to the individual Workspace accounts, nor in storage space for the school administrators and teachers. This should also refrain from sending such data as attachments in Gmail. Schools should only process and store such sensitive data in separate tools designed for school administrations. The risk of storing such data in combination with the Google Education account is that pupils may use their Google Workspace account for a long period of time. If information about undesirable behaviour, or learning difficulties is shared with future schools, all sorts of conclusions can be drawn from such data without the children and their parents being aware of it.

Risks 9-12 years

At this age, children log in and click away, usually without knowing what they are doing. They do not pay attention to the type of environment they are working in (educational or commercial). A 9-year old pupil who is presented with a pop-up window asking him/her to enter information about him/herself, will often enter the requested information quickly, without thinking about the consequences. The pupil is unable to consider alternatives, such as not visiting the website, and probably does not realise it is possible to close the pop-up window without consequences. They tend to consent to download apps, and launch applications, without a conscious decision about the impact

[33] YouTube Kids is a specific app for children, with popular children's videos and diverse new content, delivered in a way that's easy to use for children. YouTube Kids was launched in June 2021 in the Netherlands. Google, Important information for grownups about YouTube Kids, URL: https://support.google.com/youtubekids/answer/6130561 .

or consequences. Parents may use e-mail to correspond with the school about health or other sensitive personal issues.

Mitigating measures 9-12 years

Schools should prevent where possible that pupils are confronted with consent requests. They should not enable access to the Additional Services from the Google school account, as children at this age are not reading explanatory texts about choices. They will generally say Yes to any choice presented on screen, if that is the easiest way to continue with what they are doing. In this case, a choice offered by Google to use Additional Services. Children may start to create their own Google accounts. To protect these children against the risk that Google will use the data about the behaviour of the child for commercial purposes, schools should prevent pupils from using a personal Google account in school, by prohibiting simultaneous log-in with a private and a school Google account. Teachers should only use YouTube clips as embedded material in the Google Classroom (a Core Workspace Service). Similar to the advice for the age group 6-9 schools should not publish audio-visual material with identifiable children on YouTube. If the schools use Chromebooks or the Chrome browser on other school laptops or desktops, they should follow the recommended privacy protective settings in this Update report as long as Google is not yet a data processor for these services.

Risks 12-16 years

At this age, children generally do not carefully read terms and explanations about privacy choices. They are numbed by the cookie banners on every website, and just click Yes on any green button, regardless of the consequences of the default settings. At the same time, peer pressure is very strong, to use all kinds of social media with highly privacy invasive characteristics. Children often own their own smartphone, the majority Android, and generally also have access to a laptop or desktop.

Translated to Google Workspace, it is almost inevitable for children to create a private Google Account. First of all, when they use an Android device they are required to create a Google account. Second, because children want to subscribe to the YouTube feed of their favourite YouTubers, to remember videos for later viewing, to like videos and to get personalised viewing recommendations. Third, they need an account to get rid of Google's daily consent banner for Google's many services and purposes. Fourth, because children want to store their photos in Google Photos. Fifth, because they want to use Chrome Sync to have access to their full browsing and search history on different devices, and remember passwords across their devices. For children this age, the difference between what Google defines as Core Services, and what Google defines as Additional Services, is incomprehensible. Therefore, they do not distinguish between use of YouTube or Photos, and the use of Gmail and Chrome Sync.

Mitigating measures 12-16 years

Schools cannot prevent that pupils are confronted with consent requests from Google on their private devices. They can technically prevent access to the Additional Services at school, and simultaneous log-in with the private and the school account, but they cannot prevent children from creating a private account. They should explain to the children why access to Additional Services is blocked. They may consider organising an information session for the parents, to make them aware that they are responsible for providing consent to Google for such a private account, and what the privacy risks are for the children. Additionally schools should warn the children not to use Google's feedback form (even though the chance is high most children will ignore this form anyway).

The recommendations for younger age groups with regard to the use of Chromebooks, the Chrome browser, YouTube and other Additional Services also apply to this age group.

Appendix 1: list of Additional Services

The table below shows the 54 Additional Services mentioned by Google in the Admin Console with individual On or Off controls.[34] Google acts as a data controller for these services. Services frequently used by children and students are highlighted in yellow. But this is not an exhaustive list. Google also publishes a longer list of specific services that are subjected to Google's (consumer) Terms of Service.[35] That means Google acts as an independent data controller for these services. The three most relevant specific services are Chrome OS, Chrome browser, and Google Scholar.

Google Additional Services admins for Google Workspace can turn On or Off

AppSheet	Applied Digital Skills	Assignments	Blogger
Brand Accounts	Campaign Manager 360	Chrome Web Store	~~Classroom~~ [=Core Service in Education]
CS First	Developer Platform	FeedBurner	Google Ad Manager
Google Ads	Google AdSense	Google Alerts	Google Analytics
Google Bookmarks	Google Books	Google Chrome Sync	Google Cloud Platform
Google Data Studio	Google Domains	Google Earth	Google Fi
Google Groups	Google Maps	Google My Business	Google My Maps
Google Pay	Google Photos	Google Play	Google Play Console
Google Public Data Explorer	Google Search Console	Google Takeout	Google Translator Toolkit
Individual storage	Location History	Managed Google Play	Material Gallery
Merchant Center	Partner Dash	Play Books Partner Center	Programmable Search Engine
Question Hub	Scholar and Scholar Profiles	Search Ads 360	Search and Assistant
Socratic	Studio	Third-party App Backups	Tour Creator
Web and App Activity	YouTube		

[34] Google Workspace Admin Help, Additional Google services, URL: https://support.google.com/a/answer/181865?hl=en

[35] Google, Services that use Google's Terms of Service & their service-specific additional terms and policies, URL: https://policies.google.com/terms/service-specific?hl=en

Appendix 2: Chrome browser and OS

On 14 July 2021 Google provided Privacy Company with detailed information about the nature of the data collection via its browser and operating system Chrome, and the consequences of enabling or disabling certain privacy settings.

Google explains when Chrome collects personal data, and that this may include Customer Content Data if an end user uses Chrome Sync. These explanations are quoted below.

Google also provides explanations about some specific events collected from Chrome. These specific events were highlighted by Privacy Company on a longer, confidential list, to check if they would contain sensitive data. With Google's permission, the information about these specific events is included in this (public) Appendix, with an advice for admins to take central measures to mitigate the risks as long as Google does not offer a processor version of the browser and Chromebook.

Google refers to its *Chrome Privacy Whitepaper* for more information.[36]

List of some specific telemetry events Chrome browser

Name of event	Explanation	Advice admins
Spellcheck_ lookup	Chromium can provide smarter spell-checking, by sending the text that the users type into the browser, to Google's servers. This allows users to use the same spell-checking technology used by Google products, such as Docs. If the feature is enabled, Chromium will send the entire contents of text fields as user types them to Google, along with the browser's default language. Google returns a list of suggested spellings, which will be displayed in the context menu.	SpellCheckServiceEnabled: false [=disable] BrowserSignin: false [=disable]
Translate_ url_fetcher and translate requests	Chrome can provide translations for the web sites visited by the user. If this feature is enabled, Chrome sends network requests to download the list of supported languages and a library to perform translations. Current locale is sent to fetch the list of supported languages. The translation library that is obtained via this interface will perform the actual translation, and it will send words and phrases in the site to the server. Translate requests themselves are sent via Javascript injected into the website. Google does not log these requests. Google may record the following specific UMA telemetry: Sample of relevant UMA telemetry: ○ Translate.LanguageDetection.ContentLength — The number of characters of page content used for language detection. ○ Translate.MenuTranslation.IsAvailable — Logs the availability of translation from the context (Desktop) menu and app (Mobile) menu. ○ Translate.Translation.SourceLanguage — Records the source language used for a translation. ○ Translate.Translation.TargetLanguage — Records the target language used for a translation. ○ Translate.Translate — The number of times the translate button was clicked.	TranslateEnabled: false [=disable]

[36] Google Chrome Privacy Whitepaper, last modified 4 February 2021, URL: https://www.google.com/chrome/privacy/whitepaper.html

	○ Translate.Translation.Type — Records the type of translation being performed, either manual or automatic. We additionally breakdown automatic translations by the reason why an automatic translation was performed. End users can see a sample of these specific UMA telemetry data by visiting chrome://histograms.	
gcm_ checkin[37]	Chromium interacts with Google Cloud Messaging to receive push messages for various browser features, as well as on behalf of websites and extensions. The check-in periodically verifies the client's validity with Google servers, and receive updates to configuration regarding interacting with Google services. The GCM system is used both by push notifications from websites and by some Chrome features (for example, Sync) to route content to the device. An instance of a feature using the GCM system is called a "client". This event collects the IMEI and the MAC address of end user devices. However, Google assured Privacy Company it does not collect these in its own Chrome implementation. The gcm_checkin message is sent when there is an active GCM registration. On Desktop and iOS, there is only an active registration when there is at least 1 active client (whether that is because a feature using it is enabled or the user has subscribed to a push notification from a website). On Android, there is always an active registration, regardless of whether there are any active clients. This is because other apps on the device use the same registration, and therefore Chrome cannot unilaterally delete the registration.	This feature cannot be disabled in settings
lib_address	Address format metadata assists in handling postal addresses from all over the world. This request cannot include the user's home address or any other personal data. The data is only the country code for the address which the user is currently entering. For example, if a user selects "Sweden" then, regardless of whether they live in Sweden, the request will contain simply "SE" and nothing else. The endpoint for this message is the publicly-available https://chromium-i18n.appspot.com/ssl-aggregate-address , which is used by various products and can also be visited in the browser. Therefore the server does not know whether the message originated from Chrome.	This feature cannot be disabled in settings. Advice users not to edit the address in Android 'Web Payments' settings, Android's Chromium settings ('Autofill and payments' -> 'Addresses'), and Chromium settings on desktop ('Manage Autofill Settings' -> 'Addresses').
client_down load_request[38]	Chromium checks whether a given download is likely to be dangerous by sending this client download request to Google's Safe Browsing servers. Safe Browsing server will respond to this request by sending back a verdict, indicating if this download is safe or the danger type of this download (e.g. dangerous content, uncommon content, potentially harmful, etc). When Safe Browsing detects that a URL might be dangerous based on its local database, it sends a	This feature cannot be disabled in settings and does not result in a high risk. SafeBrowsingExtendedReportingEnabled to false [=disable

[37] Google refers to the .proto file for the contents of the message: https://source.chromium.org/chromium/chromium/src/+/main:google_apis/gcm/protocol/checkin.proto.

[38] The contents of this request are documented at ClientDownloadRequest message in https://cs.chromium.org/chromium/src/components/safe_browsing/csd.proto

	partial hash of that URL to Google to verify it before showing a warning to the user. This partial hash does not expose the URL to Google.	extended safe browsing]
lookup_single_password_leak	In order to inform signed-in users about leaked credentials this service uploads a prefix of the hashed username, as well as the encrypted username and password following a successful password form submission. The former is a 3 bytes of the hash and doesn't reveal the username to the server in any way. The latter is completely opaque to the server. The server responds with a list of encrypted leaked credentials matching the prefix of the hashed username, as well as with a re-encypted version of the uploaded username and password. Chrome then reverses its encryption on the re-encrypted credential and tries to find it in the list of leaked credentials. If a match is found, Chrome notifies the user and prompts them to change their credentials. Re-encryption part is for the privacy reason. The server can't read the user's password. At the same time the client can't read the usernames/passwords of other leaked accounts but only can check the current one.	[Not recommended, but possible] PasswordLeakDetectionEnabled: false
geo_language_provider and network_location_provider	Obtains geo position based on current IP address and local network information including Wi-Fi access points (even if you're not using them). For Chromebooks without GPS, location is not tied to user identity	DefaultGeolocation Setting: 2 [=disable]
rlz_ping	Used for measuring the effectiveness of a promotion. Google has explained this is a mechanism for vendors of for example Chromebooks to mention their origin. This event collects: a non-unique cohort tag of when Chromium was installed, a unique machine id on desktop platforms, whether Google is the default omnibox search and whether google.com is the default home page.	This feature cannot be disabled in settings, but admins are advised not to use Google Search as default provider
omnibox_zero suggest	When the user focuses the omnibox, Chrome can provide search or navigation suggestions from the default search provider in the omnibox dropdown, based on the current page URL. This is limited to users whose default search engine is Google, as no other search engines currently support this kind of suggestion	SearchSuggest Enabled: false [=disable]
chrome_feedback_report_app[39]	Users can press Alt+Shift+i to report a bug or a feedback in general. Along with the free-form text they entered, system logs that helps in diagnosis of the issue are sent to Google. This service uploads the report to Google Feedback server.	This feature cannot be disabled in settings, but admin should warn end users not to use this feature
new_tab_page_handler	Logs impression and interaction with doodle or promo, only on desktop. Contains a string identifying todays doodle or promo and token identifying a single interaction session. A new tab may contain thumbnails of websites that have been shown as search results in Search, even if the user has not visited that page.	DefaultSearchProviderEnabled: false BrowserSignin: false [=disable]
search_suggest_service	Downloads search suggestions to be shown on the New Tab Page to logged-in users based on their previous search history. Sends Google credentials if the user is signed in.	DefaultSearchProviderEnabled: false

[39] The contents of this request are documented at https://chromeenterprise.google/policies/#UserFeedbackAllowed

Collection of Customer Data through the Chrome browser

Google states that by default it does not process Customer Content Data through the Chrome browser. "*However, if an end user uses Chrome Sync, Google will process the following Customer Data:*

- *Installed apps and extensions, including their settings*
- *Personal autofill data (including physical addresses)*
- *Login credentials (username and password pairs)*
- *Credit card information*
- *Bookmarks*
- *Browsing history, including which webpages are currently open*
- *Local Chrome and Chrome OS settings*

Login credentials and credit card information may also be processed by Google servers if the user enables it for individual items.

If the user enables the Sync feature, Google servers will process the following personal data (excluding Customer Data mentioned above):

- *The Google Account ID*
- *Connected Wifi networks and passwords (Chrome OS only).*"

Collection of personal data through the Chrome browser

Google explains that it does not intentionally processes directly identifying personal data from Chrome users, unless they are signed in. Google does generate and process a specific identifier, the UMA client ID. If users are signed in, or use Sync, Chrome collects the Google Account ID.

By default, Google servers do not process any data that can identify the user through the use of Chrome browser. However, the user may enable features or policies that process personal data, as described below. Pseudo-anonymous data, such as the UMA client ID, are processed by Google servers but cannot be used to identify the user without the use of additional information and significant effort, so are excluded from this section.

If the user has signed in to the Chrome browser, the Google account ID will be processed by Google servers to access data previously collected by other Google products (note it is not necessary to be signed in to use Chrome browser).

If Chrome browser detects that a security incident has occurred (see Safe Browsing below), Google servers will sometimes process the current webpage's URL, which may contain personal data. This occurs more often if Safe Browsing Extended Reporting has been enabled by the user. This feature can be completely disabled by an administrator by setting the policy SafeBrowsingExtendedReportingEnabled to false.[40] *This feature can be enabled for all users by setting the same policy to true. The admin selection overrides the user's selection.*

[40] https://chromeenterprise.google/policies/#SafeBrowsingExtendedReportingEnabled

If the user enables the Enhanced Spell Check feature, Google servers will process the user's text input, which may contain personal data. This feature can be completely disabled by an administrator by setting the policy SpellCheckServiceEnabled to false.[41]

If the user uses the Webpage Translate feature, Google servers will process text on the current webpage and the current webpage's URL, which may contain personal data. This feature can be completely disabled by an administrator by setting the policy TranslateEnabled to false.[42]

If the user plays DRM-protected content on a website, Google servers will process the ID of the user's device. The website will process a different ID, which is discarded if the user clears the website's cookies.

Overview of the most relevant Chrome Browser features

Google provides a list of explanations about the Chrome browser features, namely: Sync, Autofill, Password Leak Detection, Safe browsing and Browser updater, Enhanced Spell Check, Webpage Translation and DRM.

Chrome Sync

The user may optionally enable a feature where much of their local data is sent to Google servers. Other machines on which the user has also enabled Sync can download that data, so that it's consistent across all devices and the user has a seamless experience across all their machines.

When Sync is enabled, the following data is processed on Google servers:

- *Installed apps and extensions, including their settings*
- *Autofill data (see next section)*
- *Bookmarks*
- *Browsing history, including which webpages are currently open*
- *Local Chrome and Chrome OS settings*
- *Connected Wifi networks and their passwords (Chrome OS only)*
- *Usage statistics*

This data is required to provide a seamless cross-machine experience. The user can control which types of data are synced, and may exclude certain categories of data; if they do, that data will not be processed by Google servers.

The user may also optionally encrypt this data with a custom passphrase. If they do, this data is not readable by Google. If they do not, Google may process this data to provide security and personalization features to the user depending on the user's settings in their Google Account.

Chrome Sync can be completely disabled by an administrator by setting the policy SyncDisabled to true. Specific categories of data can be excluded from Chrome Sync by the administrator, by configuring the policy SyncTypesListDisabled.

Autofill

This feature remembers the user's input into forms on websites so that the same information can be automatically filled into similar forms on other websites.

---

[41] https://chromeenterprise.google/policies/#SpellCheckServiceEnabled

[42] https://chromeenterprise.google/policies/#TranslateEnabled

The following data is processed locally by the user's machine:

- *The user's name, honorific prefix, email address, phone number, and physical address*
- *The user's login credentials (username and password pairs)*
- *The user's credit card information*

If the user has enabled Sync (see above) then this data is processed by Google servers along with their Google Account ID, so that it is available on other devices. If the data is encrypted with a custom passphrase, it is not readable by Google.

If the user has signed in to the Chrome browser, the user may, optionally for each individual item, have the data processed by Google servers along with their Google Account ID, so that it is available on other devices.

Administrators may disable browser sign-in by setting the policy BrowserSignin to false, which will prevent any of this data from being processed by Google servers. Administrators may disable personal information from being processed as part of this feature by setting the policy AutofillAddressEnabled to false. Administrators may disable login credentials from being processed as part of this feature by setting the policy PasswordManagerEnabled to false. Administrators may disable credit card information from being processed as part of this feature by setting the policy AutofillCreditCardEnabled to false.

Password Leak Detection

When the user's passwords are processed as part of Autofill (see previous section), we offer additional features.

Google servers may process an encrypted version of the user's username and password pair to detect if the user's login credentials have been leaked. This data is not readable by Google. If the credential is leaked, we notify the user that they should change the affected password.

This feature can be completely disabled by an administrator by setting the policy PasswordLeakDetectionEnabled to false or by disabling the Safe Browsing feature (see next section).

Safe Browsing

This feature protects users from malicious websites. It is enabled by default, but users can optionally disable it.

When enabled, information about the user's recent activity may be processed on Google servers when Chrome detects that one of the following "security incidents" occurred:

- *The user visits a website known to be malicious.*
- *The user visits an unknown website that is likely to be malicious according to heuristics.*
- *The user enters a password on a different website than the credentials are for, and therefore may have been phished.*
- *The user downloads a file that could be malicious.*

This data is used to protect users from further malicious activity.

This feature can be completely disabled by an administrator by setting the policy SafeBrowsingProtectionLevel to NoProtection. An administrator can prevent users from disabling the feature by setting the same policy to StandardProtection.

Safe Browsing Extended Reporting
The user may optionally enable a mode where Chrome will allow Google to process additional data in order to provide additional protection from malicious websites.

When enabled, the following changes are made from the standard Safe Browsing feature:

- *When a security incident occurs, the user can optionally amend their recent activity to include their recent browsing history.*
- *The user's recent activity may also be processed by Google servers when the user visits an unknown website that might be malicious according to heuristics.*
- *Information about a website that the user is currently typing a password into may be processed by Google servers, in order to proactively prevent the user from being phished.*

This data is used to protect users from further malicious activity.

This feature can be completely disabled by an administrator by setting the policy SafeBrowsingExtendedReportingEnabled to false. This feature can be enabled for all users by setting the same policy to true. The admin selection overrides the user's selection.

Browser Updater
The browser regularly installs new versions of itself by contacting Google servers.

The following data is processed by Google servers to provide updated Chrome files:

- *Information about the currently-installed version of Chrome browser*
- *Information about the computer's hardware and OS, including whether the computer is managed by an administrator*
- *Days since the last successful install*
- *A random number that is never reused*
- *Usage statistics, including whether the install succeeded or not*

This data is used to ensure the correct files are downloaded given the user's hardware and OS, and to detect duplicate requests.

When using Chrome browser on Chrome OS, no IDs are processed as part of this feature.

This feature can be completely disabled by an administrator by setting the policy DeviceAutoUpdateDisabled to true. Updates can be restricted to particular versions of Chrome by setting the DeviceTargetVersionPrefix policy. The rate at which updates are applied can be controlled by setting the DeviceUpdateStagingSchedule policy.

Enhanced Spell Check
The user may optionally enable a mode where any text they type is sent to Google for intelligent spell checking. When disabled, all processing is done by the user's local machine.

When enabled, the following data is processed by Google servers:

- *The user's text input*
- *Whether the user accepts or ignores suggestions*
- *Chrome's guess about what language the text is in*
- *An identifier that Chrome discards after less than 1 day*
- *Usage statistics*

The data is used to respond with spelling suggestions, and to ensure we remember the user's previous decisions for a short time.

This feature can be completely disabled by an administrator by setting the policy SpellCheckServiceEnabled to false.

Webpage Translation
This feature allows the user to automatically translate webpages to another language. The browser will proactively offer this feature to users when they visit a site that is written in a language other than their browser's configured language.

When used, the following data is processed by Google servers:
- *The text on the page*
- *The URL of the page*
- *The source and target languages*
- *Usage statistics*

This data is used to provide the translated text, which is rendered by the user's local machine.

This feature can be completely disabled by an administrator by setting the policy TranslateEnabled to false. Users can switch this on or off through the Chrome Browser.[43] The admin selection overrides the user's selection.

DRM
This feature allows the browser to play high-resolution videos and other content that websites make available only in an encrypted fashion ("DRM-protected content").

When the user tries to play DRM-protected content, the ID of the user's device is processed on Google servers. This is used to block devices that have been used to crack DRM protection.

When the user tries to play DRM-protected content, the browser generates a new ID that is sent to the website. This ID is used by the website to ask Google whether the device is legitimate. This ID will be discarded if the user clears the website's cookies.

Users can disable this feature in browser settings. Administrators are not able to control this feature.

[43] https://support.google.com/chrome/answer/173424