PRIVACY COMPANY

Verification report Processor version Google Chrome for Education

SIVON, 7 March 2024

Public version

By Floor Terra and Sjoera Nas
senior advisors Privacy Company

Version management

Version	Date	Remarks
0.1	8 December 2021	Outline with questions
0.2	12 September 2022	First rough draft, completed intro, Q1 and Q6
0.3	14 September	First completed draft
0.4	26 September	Input SIVON and SURF processed with track changes
0.5	29 September	Clean version
0.6	December 2022	Review version
0.7	31 January 2023	Updated report
0.8	17 March 2023	Last input Google about confidentiality processed with comments
0.9	17 March 2023	Compare 0.7 and 0.8 with track changes
1	17 March 2023	Clean version
1.1	29 June 2023	Revision based on new ChromeOS Agreement for the Dutch Education Sector 30 March 2023 - with track changes
1.2	29 June 2023	Clean public version
1.3	21 December 2023	New public verification report processor version
1.4	21 February 2024	Track changes update with the final input from Google
1.5	21 February 2024	Semi-final version shared with Google
1.6	7 March 2024	Track changes after confidentiality check Google
1.7	7 March 2024	Public version

Contents

Figures

Summary

This report contains an assessment of the technical measures taken by Google to mitigate data protection risks resulting from the use of the managed Google Chrome browser and the use of a managed Google Chromebook in the Dutch education sector. The most important measure is the introduction of a processor version of the Chrome browser and Chrome OS on Chromebooks in August 2023. SIVON has published the agreed action plan with all agreed mitigating measures.[1]

On 29 June 2023, a first inspection report was completed, with a legal assessment of the new processor agreement.[2] Both the initial and this verification report on Chrome were commissioned by SIVON, the IT procurement organisation for all primary and secondary education schools in the Netherlands. SIVON worked closely with SURF, the IT procurement organisation for higher education institutions, on this verification report.

This work follows from earlier DPIAs on Google Workspace. After negotiations with Google, and a prior consultation of the Dutch Data Protection Authority, an Update DPIA report was published in August 2021. Agreement was reached with Google on a set of contractual, organizational, and technical measures to mitigate the 8 identified high data protection risks. An important highlight was Google's commitment to develop a processor version of managed Chrome browser on the managed ChromeOS by August 2023.

Prior to the release of the new software versions, Google and the Dutch education sector signed a new ChromeOS Agreement. Google also published a *Data Processing Amendment to Chrome Agreements*.[3] Based on this agreement, Google acts as data processor for the *Essential Services* in Chrome, with a limited list of permitted purposes for further processing by Google as controller (identical to the Workspace data processing agreement). Google continues to act as data controller for the *Optional Services* in Chrome.

This verification report contains the outcomes of the testing of the new processor ChromeOS and assesses if the new processor-version factually complies with the agreed action plan and mitigates the identified data protection risks. This report does not assess other data protection risks, for example, related to data transfers to third countries.

[1] SURF and SIVON, Final improvement plan Google ChromeOS and Chrome browser on Chrome devices, June 2023, URL: https://sivon.nl/wp-content/uploads/2023/07/Improvement-plan-Google-for-ChromeOS-on-managed-devices.pdf.
[2] Privacy Company for SIVON, Inspection results Google Chrome for Education, 29 June 2023, URL: https://sivon.nl/wp-content/uploads/2023/07/20230629-Chrome-inspection-report-v1-2-public-NEW.pdf .
[3] Google, Data Processing Amendment to Chrome Agreements, Last modified 16 February 2023, URL: https://www.google.com/chrome/terms/dpa_terms.html.

Six verification questions

To verify the adequacy of the technical measures taken by Google to mitigate data protection risks resulting from the use of the managed Google Chrome browser and the use of a managed Google Chromebook in the Dutch education sector, this report is based on the following six questions.:

1. Does Google offer the processor Chrome browser and Chrome OS to Dutch schools?
2. Do the three new tools for admins in ChromeOS data processor mode (domain wide Takeout, individual Service Data download and deletion of individual user data) enable schools to reply in full to Data Subject Rights Requests for the Chrome processor OS and browser data? Did Google indeed become a data processor for the individual Content Data Takeout? Is essential information missing from the output of these tools compared to the performed test scenarios?
3. Does Google's public documentation about the data types collected by the Chrome processor OS and browser enable schools to adequately inform end-users?
4. How effective are the privacy-friendly settings in the Chrome browser in blocking third-party cookies?
5. Can admins effectively block the Optional Services and web app store for which Google remains a data controller?
6. Can schools use the managed Google Play store on the managed processor-Chromebooks without data protection risks?

Outcomes

The answer to the **first question** is Yes, Google did launch a processor version of the ChromeOS on managed Chromebooks for Dutch schools in mid-August 2023.

The answer to the **second question** is Yes, taken together, Google's new tools seem sufficient to provide adequate replies to data subject access and deletion requests from end users of the managed processor ChromeOS and browser. This section contains most of the technical analysis, performed in December 2023.

The original Chrome inspection report (June 2023)[4] concluded that Google (at the time, as data controller) did not provide an adequate or timely reply to a Data Subject Access Request (DSAR) for the Chrome data. As a processor, Google agreed to develop three new features (for Workspace for Education and the managed processor Chrome browser and OS):

1. Service Data Downloader and Diagnostic Information Tool
2. Domain-wide Takeout tool for admins
3. User data deletion tool

[4] See footnote 2.

Google has developed and documented these features. Additionally, Google factually acts as data processor for the individual Takeout tool for end users.

The **third question**, about the available public documentation, can also be answered with a Yes, Google did make new documentation available, also about the Telemetry Data Google collects in via Chrome, but admins have to click on hyperlinks in the documentation about each Essential Service to see details of the data processing.

As a processor, Google agreed to publish new documentation to help schools comply with their data processing transparency obligations, and specifically, for school admins to answer data subject requests from students. Specifically, Google agreed to publish:

1. Documentation what data types are collected by which service, and
2. Documentation what categories of personal data, relating to what service, are available in the event logs for admins

Google did not create a separate page with an overview of the Chrome browser and OS telemetry events, as Google did for Workspace.[5] To mitigate the risk of the lack of transparency, SIVON has published an overview page with all Google's relevant sources of information about the data processing.[6]

The **fourth question** asked if admins could enforce privacy friendly settings in the managed Chrome browser. The answer is Yes, admins can centrally block third party cookies in the managed Chrome browser. However, they cannot block Google cookies, as these cookies are inextricably linked to the use of the Google Workspace for Education account. Because Google now acts as processor for both the ChromeOS and browser and the Workspace for Education account, there should not be any data leakage anymore to Google as data controller. As processor Google is not allowed to use its own cookies (such as the NID-cookie) for advertising purposes.[7]

Regarding the **fifth question**, the answer is that admins can effectively block the Optional Services on the managed Chromebooks for which Google is a data controller. Google has changed its role for some Optional Services, so that it processes data relating to SafeSites and SafeSearch as a data processor.

---

[5] Google, Diagnostic Information Tool, Guide for Google Workspace administrators, undated, page last visited 21 February 2024, URL: https://support.google.com/a/answer/12830816

[6] SIVON, Uitleg transparantie gegevensverwerkingen Google Workspace for Education, URL: https://sivon.nl/uitleg-transparantie-gegevensverwerkingen-google-workspace-for-education/ .

[7] Google's use of the NID-cookie was flagged as a risk in the report with 5 new findings related to Workspace for Education. Google has mitigated this risk. The updated report of new findings will be published simultaneously with this report.

The answer to the **sixth question** is No, admins should continue to block the use of managed Google Play, as Google continues to act as data controller for all metadata relating to the use of the managed Play Store. Google only processes the Content Data as a processor, such as reviews of apps. Google does not provide specific information about the data it processes through its app store. The lack of transparency, combined with the lack of purpose limitation because Google acts as a data controller, result in a lack of control for the schools and universities. To mitigate this risk schools must continue to block access to both the managed and unmanaged Play Store, as well as the Chrome webstore.

Conclusions

The table below shows if Google has mitigated the known risks by highlighting the measure in green. If Google has not taken measures, these rows are highlighted in orange. Because schools can take measures to mitigate these risks, there are no more known high risks if schools implement all recommended measures.

Table 1: Combined results of the initial inspection and this verification report

Issue	Recommended mitigating measures schools	Mitigating measures taken by Google
DSAR results incomplete	Continue to block access to the Chrome Web Store and the Google Play Store.	Commitment to do an individual assessment of each DSAR
	Use the guidance from SIVON to inform students how to request access with the school, and with Google.	Google is a processor for the Domain-wide Takeout tool for admins
		Google is a processor for the individual Takeout tool for end users
		Google has published documentation what Diagnostic / Telemetry Data the Essential Chrome Services collect, in many different help articles, per Chrome service, to the extent they collect user or device associated data at all. The help articles can be accessed through hyperlinks in the list with Essential and Optional Chrome Services.
		Google has published more information about the data retention of Chrome data in a help article about Workspace data retention.
		Google has developed a Service Data Downloader for admins
DSAR refusal explanation insufficient	Use the available admin event logs to provide access to personal data.	The managed ChromeOS includes services to access the data such as the Service Data Downloader and Diagnostic Information Tool (DIT, a Telemetry Data viewer developed for Workspace)
		Google has published an improved explanation why it may refuse access to some personal data.
		Google has published documentation what categories of personal data, relating to what service, are available in the event logs for admins.
Lack of purpose limitation data Takeout tool	Keep on disabling the Workspace *Additional Services*.	Google has become a data processor for the admin and end user Takeout tools.
Lack of purpose limitation	Sign-up for the new ChromeOS and browser processor agreement.	The processor agreement for the managed ChromeOS and browser contains two limitative lists of purposes,

ChromeOS and browser	Do not enable the *Optional Chrome Services*, for which Google continues to act as controller (already disabled for new customers).	for Google as processor, and for agreed further processing by Google as controller for its legitimate business purposes.
	Select the K-12 setting (also universities) to block processing for commercial purposes such as group profiling in Privacy Sandbox and the presentation of surveys by default.	
Lack of purpose limitation Sync data outside of Workspace for Education	Though the lack of purpose limitation is solved, schools are still advised not to enable Chrome Sync if the users are allowed to use the Google accounts for private purposes – due to transfer risks.	Based on the processor agreement for the managed ChromeOS and browser, Google is a data processor for Chrome Sync, both for the Content and Diagnostic Data (separate from Workspace for Education, where Sync is already a processor service).
Lack of purpose limitation (Managed) Play Store and Chrome Webstore	Disable access to all *Additional Services* in Workspace, including the (managed) Play Store and the Chrome Webstore. If schools wish to enable students to use selected allowed apps, they must distribute these apps via their own network. For browser extensions they can apply Force install, without users having to visit the Chrome webstore.	Google has not announced any measures.
No valid ground for transfer of personal data to the USA	Sign up for the new processor agreement and apply all data minimisation measures from the updated guidance from SIVON including all steps in the manual	Google has become a data processor for the managed ChromeOS and browser. The Dutch education customers rely on appropriate transfer mechanisms under Chapter V GDPR.
	Disable SafeSites with a registry setting (consider use of a third party filter).	Google has not replied to the request to allow for local filtering instead of transferring URLs to the USA with the IP addresses.
	Schools must centrally enforce all privacy-friendly settings, including disabling of access to google.com and youtube.com, either by enforcing use of a proxy server to block functionality on the local network, or through manual URL blocking options in the admin console.	Google offers central admin management options for the guest mode on managed Chromebooks, including blocking of third party cookies.
	Schools are (still) advised not to enable Chrome Sync if the users are allowed to use the Google accounts for private purposes, including private e-mails and private surfing behaviour from which special categories of data may be inferred – due to the risk of unauthorised access by government authorities in 7 third countries	Google makes onward transfers of the personal data to 7 third countries. The Dutch education customers rely on appropriate transfer mechanisms under Chapter V GDPR It follows from the DTIA performed for Google Workspace Meet that transfer of special categories of data leads to a high risk if schools cannot encrypt these data with a locally held key.
	Disable Sync by setting the policy *SyncDisabled* to *true* or ensure that students use a self-managed local passphrase to encrypt the Sync data	Google has not yet developed a policy for admins to centrally enforce use of encryption of the Chrome Sync data with locally held keys, in the end user devices.
Privacy unfriendly default settings	Enforce the recommended privacy-friendly settings whenever possible.	Privacy Sandbox trials are disabled for users under 18.
		Google has not responded to the request to improve the tracking protection features in the Chrome browser when third party cookies are blocked, the DNT signal is enabled and website preloading is disabled. For example, by blocking traffic to Google services where Google does not act as data processor

		(such as analytics and fonts). Google explains that admins can use policies to restrict cookies and javascript from any third party, including Google.
	Disable the Privacy Sandbox for all users (already disabled if schools follow the advice to select the K-12 setting	Google has given admins controls to block ads personalisation and measurement as part of Privacy Sandbox in the processor version of managed ChromeOS.
Lack of transparency	Disable access to the (managed) Play Store and Chrome Webstore.	Google has not announced any measures.

Introduction

This verification report on the data protection risks of the use of the Google Chrome browser and the use of a Google Chromebook is a second follow-up on the *Data Protection Impact Assessment* (DPIA) performed on the use of Google Workspace for Education. This report was commissioned by SIVON, the IT procurement organisation for all primary and secondary education schools in the Netherlands.

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 4 of the 36 government-funded universities of applied sciences, according to questionnaires from SURF and SIVON in the summer of 2021. It is plausible that schools that have procured Chromebooks, also use Google Workspace for Education, and the Chrome browser, as these tools are available by default on a Chromebook. In fact, Google uses the word Chrome to describe both the browser and the operating system and only has one version number. The ChromeOS (operating system) has a few more options than the Chrome browser: for example, access to applications from Google's Play Store.

The original DPIA on Google Workspace, commissioned by the Dutch universities HvA and RUG, was completed in June 2020, updated in March 2021, and published in May 2021.[8] After negotiations with Google stalled, the Dutch Data Protection Authority was asked for a prior consultation. In June 2021 the Dutch Data Protection Authority (Autoriteit Persoonsgegevens) warned schools and advised the responsible two ministers for Education to stop using Google Workspace before the start of the new schoolyear, 21 Augustus 2021, if the problems could not be solved.[9] Soon after, an agreement was reached with Google on a set of contractual, organizational and technical measures to mitigate the 8 high data protection risks. The Update DPIA report was published in August 2021 with a summary of the results of the negotiations.[10]

Three key highlights of this agreement are:

1. Google contractually agreed to act as data processor for the Diagnostic Data about the individual use of the services by the start of the new school year (21 August 2021), with a

[8] 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.surf.nl/files/2021-06/updated-g-suite-for-education-dpia-12-march-2021.pdf

[9] Letter from both ministers of Education to the Lower House, 8 June 2021, with two attachments: (i) the letter sent by the Dutch Data Protection Authority to SURF and SIVON, and (ii) 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

[10] Update DPIA report Google Workspace for Education, 2 August 2021, URL: https://www.sivon.nl/app/uploads/2021/08/Update-DPIA-report-Google-Workspace-for-Education-2-augustus-2021.pdf

contractual permission to 'further' process some Diagnostic Data as independent data controller, to the extent necessary, for certain agreed and limited purposes.

2. As a data processor, Google may only process the personal data for three predefined instructed purposes.
3. Google committed to develop a processor version of managed ChromeOS, and a separate processor version of the Chrome browser on managed ChromeOS. Since this could take Google 2 years, the Update DPIA already provided risk-mitigating technical measures for the schools and universities. SURF and SIVON published technical manuals for the system administrators to apply the most privacy-friendly settings to the managed Chromebooks.

The 2021 Update DPIA 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 2021 Update DPIA describes the risks for three age groups of children in more detail (ages 6-9, 9-12 and 13-16), and how the recommended measures mitigate the specific age-related risks. These assessments are not repeated in this report. SURF and SIVON have published technical manuals for the system administrators to apply the most privacy-friendly settings in Google Workspace for Education[11], and for the Chrome browser.[12] Based on feedback from the schools they regularly provide updates.[13]

In August 2023, SURF and SIVON published a verification report on the measures taken by Google to mitigate risks for Workspace for Education.[14] This report did not include a data transfer risk assessment. This assessment is performed in a separate Data Transfer Impact Assessment. SURF and SIVON will publish this DTIA with an updated version of the verification report, together with this report on Chrome.

On 29 June 2023 a first Chrome inspection report was completed and published, with a legal assessment of the new processor agreement.[15] At the time, the processor version of the Chrome browser and OS were not yet released, and could not be tested. This verification report contains the technical analysis of the new ChromeOS and browser processor versions. These assessments do not address possible data transfer risks. Transfer risks are separately addresses in a Data Transfer Impact Assessment for Google Meet, a Core service in Google Workspace for Education for which Google is a processor. SURF and SIVON will publish this DTIA together with this report, and updates on Google Workspace for Education.

---

[11] In Dutch: SURF and SIVON, Technische handleiding voor Google Workspace for Education, URL: https://sivon.nl/wp-content/uploads/2023/07/Technische-handleiding-voor-Google-Workspace-for-Education-v2.pdf.
[12] In Dutch: SURF and SIVON, Chrome privacy handleiding, URL: https://sivon.nl/wp-content/uploads/2023/09/Handleiding-ChromeOS-en-Chrome-browser.pdf .
[13] SIVON, Alles over de DPIA's op Google Workspace & ChromeOS,.URL: https://sivon.nl/alles-over-de-dpias-op-google-workspace-chromeos/ .
[14] Privacy Company for SURF and SIVON, Verification report Google remediation measures Workspace for Education, 24 July 2023, URL: https://sivon.nl/wp-content/uploads/2023/07/20230724-clean-Workspace-for-Education.pdf.
[15] Privacy Company for SIVON, Inspection results Google Chrome for Education, 29 June 2023, URL: https://sivon.nl/wp-content/uploads/2023/07/20230629-Chrome-inspection-report-v1-2-public-NEW.pdf

Scope of this report

In the previous verification report, use of the Chromebooks was tested with Microsoft Office-for-the-Web applications, to test the data protection risks if Chromebooks were used without using a Google account. This test was not repeated, as Google had agreed to become a processor both for Google Workspace for Education, and for the ChromeOS and browser. Since Google did launch the Chrome processor version as agreed, it was no longer necessary to look for an alternative provider of productivity apps that was willing to process the personal data as data processor.
This report does not repeat the legal analysis of the first verification report, nor the findings of the earlier DPIAs, or the mitigating measures recommended since August 2021[16], such as for example, disabling *Additional Services* in Google Workspace, and disabling Google Search as default search engine in Chrome. This report describes how effective Google's new processor version of the Chrome browser and ChromeOS is in mitigating data protection risks related to transparency, purpose limitation and the exercise of data subject rights.

Six questions

To verify the adequacy of the technical measures taken by Google to mitigate data protection risks resulting from the use of the managed Google Chrome browser and the use of a managed Google Chromebook in the Dutch education sector, this report is based on the following six questions:

1. Does Google offer the processor Chrome browser and Chrome OS to Dutch schools?
2. Do the three new tools for admins in ChromeOS data processor mode (domain wide Takeout, individual Service Data download and deletion of individual user data) enable schools to reply in full to Data Subject Rights Requests for the Chrome processor OS and browser data? Did Google indeed become a data processor for the individual Content Data Takeout? Is essential information missing from the output of these tools compared to the performed test scenarios?
3. Does Google's public documentation about the data types collected by the Chrome processor OS and browser enable schools to adequately inform end-users?
4. How effective are the privacy-friendly settings in the Chrome browser in blocking third-party cookies?
5. Can admins effectively block the Optional Services and web app store for which Google remains a data controller?
6. Can schools use the managed Google Play store on the managed processor-Chromebooks without data protection risks?

[16] See the manual in Dutch published by https://sivon.nl/wp-content/uploads/2023/09/Handleiding-ChromeOS-en-Chrome-browser.pdf. https://privacycompany-my.sharepoint.com/personal/sjoera_nas_privacycompany_nl/Documents/Documenten/SIVON/SIVON

Methodology and test settings

Privacy Company tested the data processing between 20 November and 6 December 2023 with the following set-up:

- A paid license was procured for Google Workspace for Education Plus, with the Chrome Enterprise upgrade, by the existing primary school CNS Ede (Stichting Christelijk Nationaal Schoolonderwijs). For this test, the specific domain cnsede-test.nl was created and used.
- Two Google Workspace for Education accounts were created, floor@cnsede-test.nl and floor2@cnsede-test.nl.
- The Google Workspace for Education license was configured for a K-12 school (pupils younger than 18 years).
- One Chromebooks was used: A Lenovo Chromebook S330 with ChromeOS 118.0.5993.124.[17]

The device was configured as recommended by SIVON, with privacy-friendly settings.

To quickly test the new processor version, all the available settings for admins, and some specific options for end-users were studied. Because Privacy Company worked in an existing school test-tenant, a separate effort was made to figure out the default options.

To answer the 6 questions, different activities were performed.

1. Looked up availability of the new processor version, and record all available legal texts and hyperlinks.
2. Tested some functionalities such as bookmark syncing, password syncing, visited some websites to test the new takeout possibilities (not a retest of Safe Browsing or Safe Sites), and used the three new takeout options. The results were viewed, and screenshotted for this report, in Visual Studio Code.
3. Privacy Company searched for public information about the event logs Google collects via the ChromeOS and browser, as well as the Chrome Telemetry events. Due to certificate pinning of the Play store elements that run locally on the Chromebook (and are not disabled when a school disables the Play Store, as recommended by SIVON), it was not possible to intercept all outgoing traffic. The intercepting proxy often had to be disabled for the Chromebook to function. Therefore, it was difficult to compare the network traffic from the tests with the public documentation. Retested with 3 settings changed: Translate, Spellcheck and Browser sign-in.
4. Visited one media website, nu.nl, that carries a lot of tracking cookies. Privacy Company gave consent for tracking cookies in the cookie management banner from the website, to test if the Chrome setting to block tracking cookies overruled this user consent.

[17] Google ChromeOS, ChromeOS 118 release notes, URL: https://chromeos.dev/en/posts/chromeos-118-release-notes. Google explains this version reached stable release on 17 October 2023.

5. Tested the available admin options to block Optional Services, including the Web App Store.
6. Inspected the available legal terms in the admin console, to check if Google had classified the managed Play Store as Essential (processor) Service.

The activities were performed **on a managed school Chromebook** (this automatically means the **Chrome browser is also managed**). While the activities were performed, the outgoing data traffic was intercepted with mitmproxy, where possible.[18]

Privacy Company ensured that the research is reproducible and repeatable. Screenshots were made to evidence relevant changes or documentation. All data have been recorded.

[18] In the most recent test Privacy Company used mitmproxy version 10.0.0.

1. Processor Chrome browser and Chrome OS

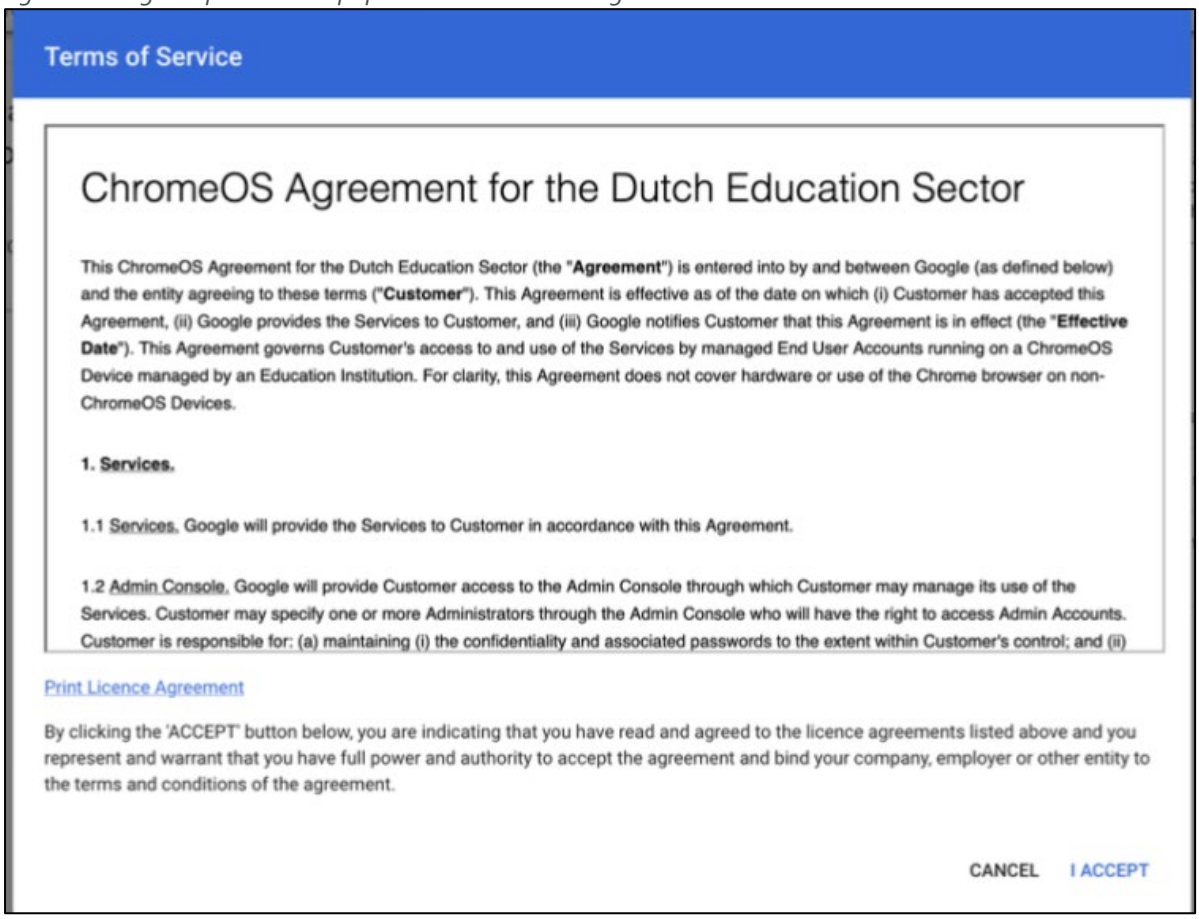
This section answers the first question:

Does Google offer the processor Chrome browser and Chrome OS to Dutch schools?

1.1 Findings

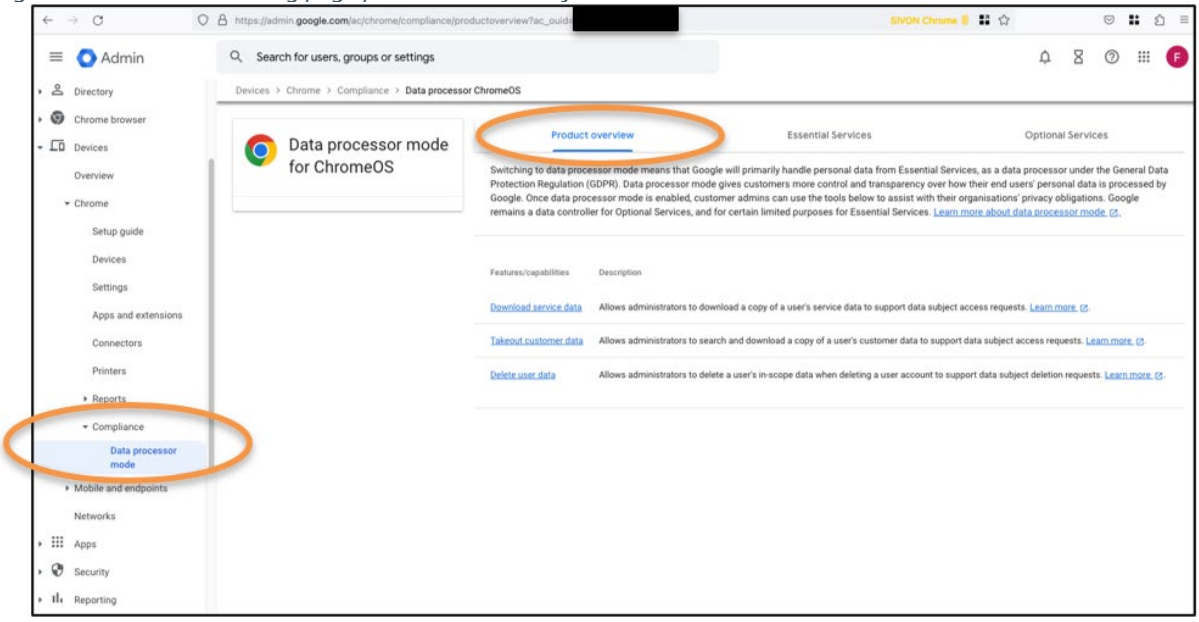
As tested by Privacy Company on 20 November 2023 in the test tenant of a primary school, Google offers a processor version of the ChromeOS and Chrome browser to Dutch schools. The new processor mode currently is only available for Dutch schools.[19] Admins are first asked to accept the processor mode (See Figure 1 below) and can than access a new Chrome landing page in the general Google Admin Console. See Figure 2 below.

Figure 1: Google request to accept processor ChromeOS Agreement



[19] Google publishes a list of EU countries where the processor services are available. This page only mentions the Netherlands (page last visited 21 February 2024), URL: https://support.google.com/chrome/a/answer/14294567?sjid=7817823478896445101-EU.

Figure 2: New admin landing page processor version of ChromeOS and Chrome browser



For all other customers, Google continues to process the Chrome personal data as data controller. This role as controller follows from Google's (general) Terms of Service that Google's general (consumer) Privacy Policy applies to the data processing by Chrome and the ChromeOS. This Privacy Policy contains 33 purposes. These 33 purposes are included and assessed in the Google Workspace DPIA.[20] Additionally, Google's Chrome Privacy Notice contained 16 other purposes for the data processing.[21] As shown in Figure 3 below, this separate Chrome Privacy Notice is no longer available.

Figure 3: Chrome Privacy Notice no longer available[22]

The Chrome Privacy Notice is no longer available.

Your personal information will continue to be used and protected in accordance with the Google Privacy Policy.

The Chrome Help Center now has a "Privacy in Chrome" section with articles organized by topic. These articles provide details on how to manage information collected, stored, and shared when using Chrome.

To provide feedback, follow these instructions.

In the test tenant, Google's general Terms of Service for Workspace for Education are not available. Instead, Google refers to an offline variant of this Agreement. See Figure 4 and Figure 5 below.

[20] 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, page 93-95, URL: https://www.surf.nl/files/2021-06/updated-g-suite-for-education-dpia-12-march-2021.pdf

[21] Google Chrome Privacy Notice last modified 11 August 2022, no longer available. Google now refers to its general Privacy Policy.

[22] Idem.

Figure 4: Google Workspace for Education Terms of Service

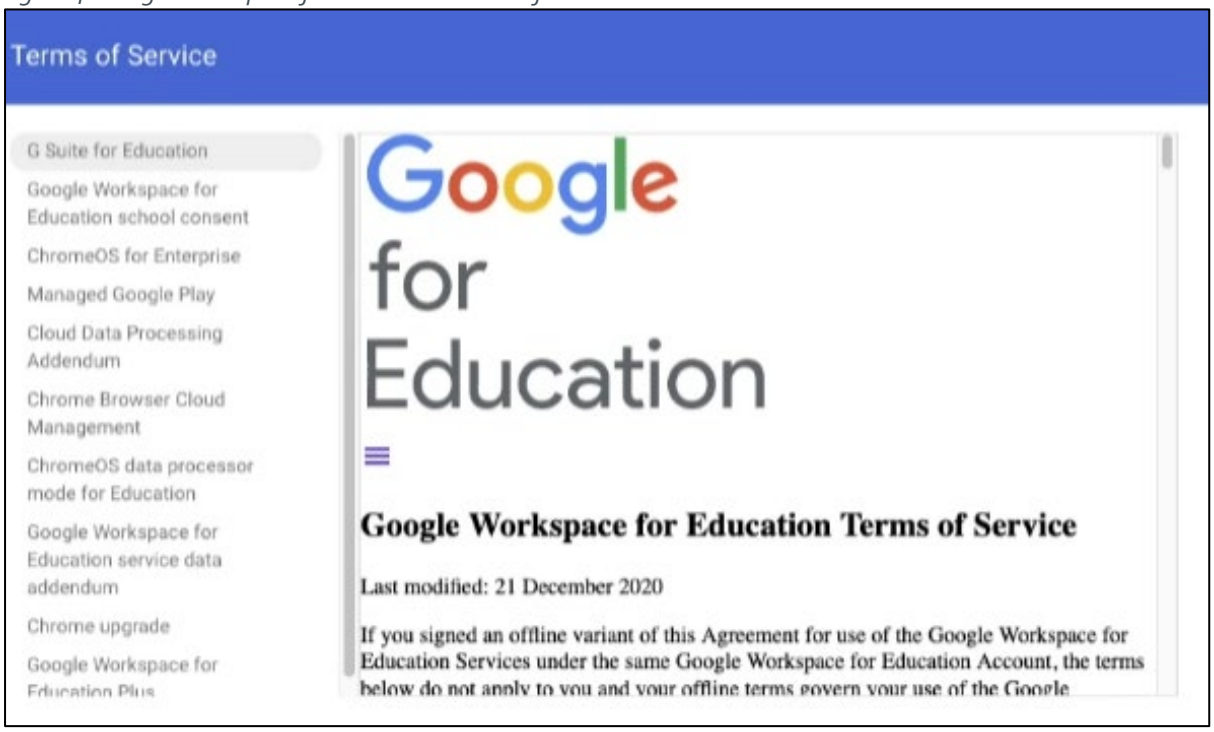
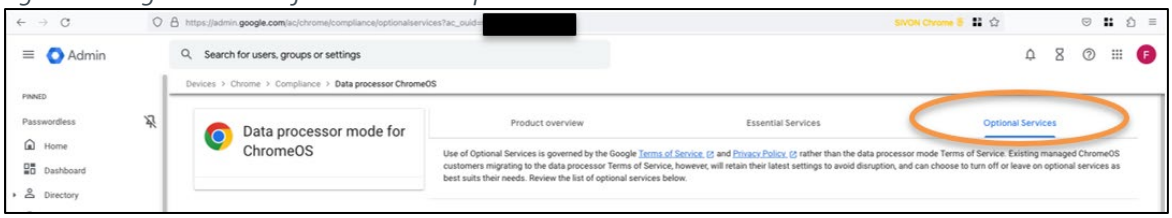


Figure 5: Reference to offline variant, available through SIVON

Google offers two distinctive lists of services to Dutch school admins for Chrome in processor mode: a list of Essential (processor) services, and a second list of Optional (controller) Services. See Figure 6 below. Section 5 of this verification report describes the contents of the Optional Services, and if admins can effectively block access to these controller services.

Figure 6: Google overview of Essential and Optional Services



As mentioned in the June 2023 legal assessment, the data processing agreement for the managed ChromeOS and browser contains two limitative lists of purposes, for Google as processor, and for agreed further processing by Google as controller for its legitimate business purposes. As shown in Figure 7, Google explains these conditions in a new Help article for admins of Dutch schools.

Figure 7: Google explanation about the purposes of the processing[23]

Your data

Essential Services

When providing Essential Services, Google may only process personal data contained in Customer Data (also known as Customer Personal Data), and Service Data (data generated by Google when Essential Services are used) as permitted in the data processor mode Terms of Services.

When Google processes personal data under these services, it can only be to:

1. Provide, maintain, and improve Essential Services,
2. Identify, address, and fix security threats, risks, bugs and other anomalies, and
3. Develop, deliver, and install updates to the Essential Services.

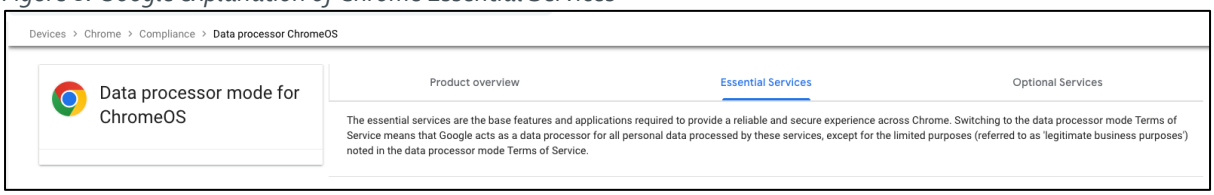
These three processing purposes are called the **Customer Instructions**.

Service Data may also continue to be processed by Google as a data controller only for specific, limited, purposes detailed in the agreement, known as **Legitimate Business Purposes**. Examples include billing and account management, technical support, or abuse detection.

Google describes that the list of Essential Services contains the base features and applications required to provide a reliable and secure experience across Chrome. Google also explains that the contractual terms allow Google to 'further' process some personal data, when necessary, for a limitative list of controller purposes. See Figure 8 below.

[23] Google ChromeOS data processor mode- Overview for enterprises (only for managed ChromeOS devices in the Netherlands), undated, page last visited 21 February 2024, URL: https://support.google.com/chrome/a/answer/13816756 .

Figure 8: Google explanation of Chrome Essential Services



Google lists 35 Essential Services, as listed in Appendix 1.[24] Google also publishes a help article with an overview.[25] All of these services used to be controller-services, as part of the use of Google's controller services ChromeOS and Chrome browser. The new Chrome processor module in the Admin Console contains many options for admins to selectively disable Essential Services. Such disabling may be necessary to mitigate possible data transfer risks. This is outside of the scope of this report.

[24] Google Chrome Enterprise and Education Help, List of Essential Services, undated, page last visited 21 February 2024, URL: https://support.google.com/chrome/a/answer/13598068

[25] Chrome Enterprise Essential Services in data processor mode on managed ChromeOS devices, undated, page last visited on 21 February 2024, URL: https://support.google.com/chrome/a/topic/13597460?sjid=7817823478896445101-EU

2. New Takeout and deletion tools

This section answers the second question:

Do the three new tools for admins (domain wide Takeout, the individual Service Data download and deletion of individual user data) enable schools to reply in full to Data Subject Rights Requests for the Chrome processor data? Does Google indeed act as processor for the individual Content Data Takeout?

2.1 Findings

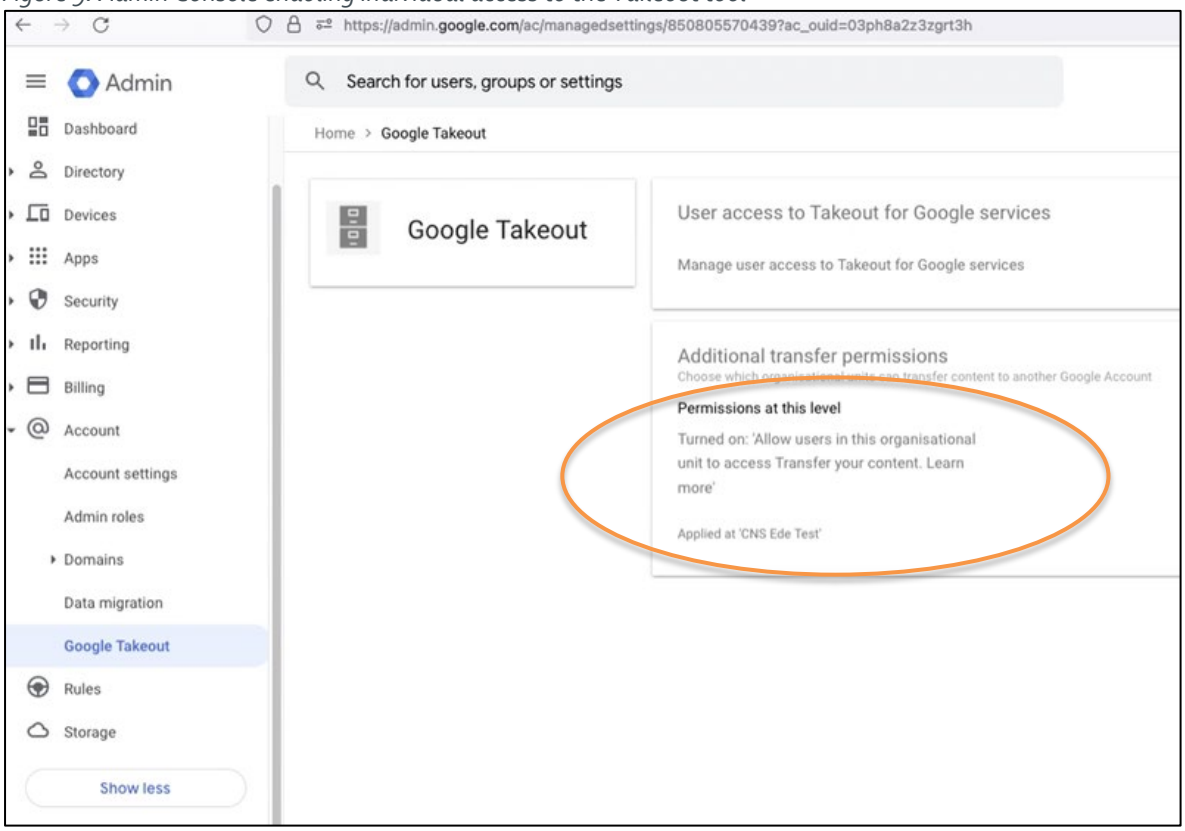
As shown in Figure 10 below, Google offers three tools to admins to fulfil data subject requests.

1. The Download Service Data option contains user-email or device serial number-keyed Service Data, including Chrome Sync data. Google committed to develop this tool to: "*include data from server generated service logs, and data sent from the end user device as Telemetry Data.*"
2. The Takeout Customer Data (also called *Domain-wide Takeout* by Google) option contains user-email keyed Content Personal Data from Chrome/OS services that Google processes as data processor (i.e., *Essential Services*). Google committed to develop this tool to: "*include user content data from Google Play, but not any Diagnostic Data.*"
3. The Delete User Data option enables admins to delete individual user data, and the available information in the audit logs (called event logs by Google).

There is a fourth tool for end users of the processor ChromeOS and browser to obtain access to their personal data, as a kind of self-service data subject access request, the individual Takeout tool.

This tool allows students to export copies of Content Data and some Diagnostic Data to a local zip folder. As shown in Figure 9 below, admins can enable use of this tool for end users.

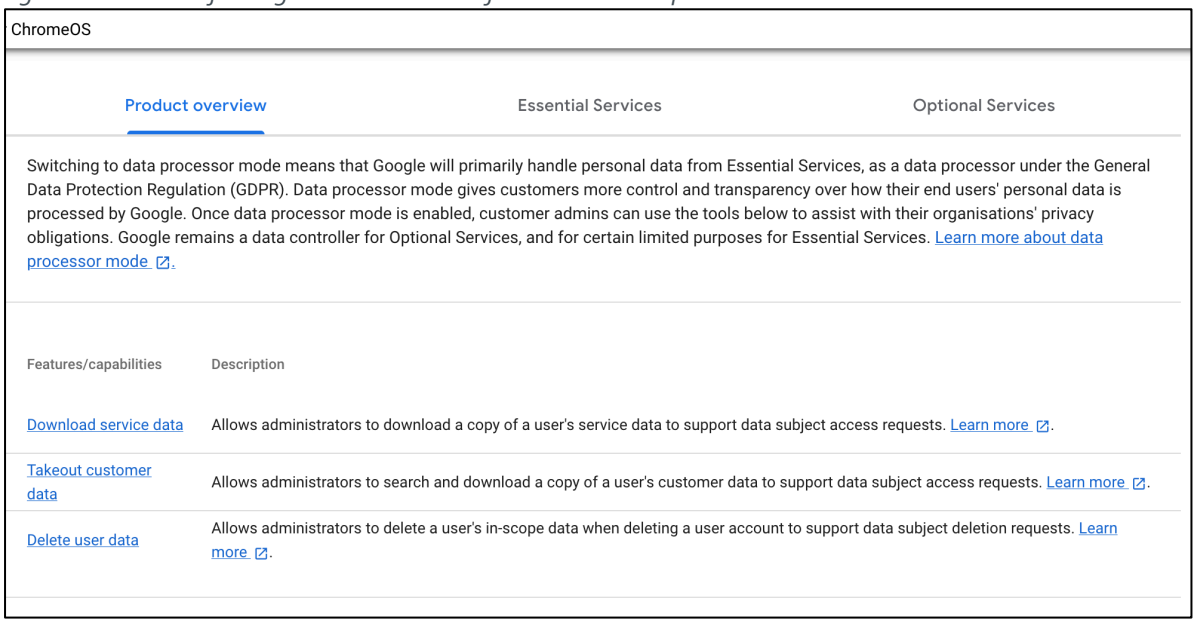
Figure 9: Admin Console enabling individual access to the Takeout tool



The Takeout tool used to be an *Additional Service*, with Google as data controller. Therefore, schools were advised to disable this feature. However, in June 2023 Privacy Company retested in the managed ChromeOS of the test tenant, and established that Takeout was no longer part of the *Additional Services*. Therefore, admins can safely enable individual access to this tool, as shown in Figure 9 above.

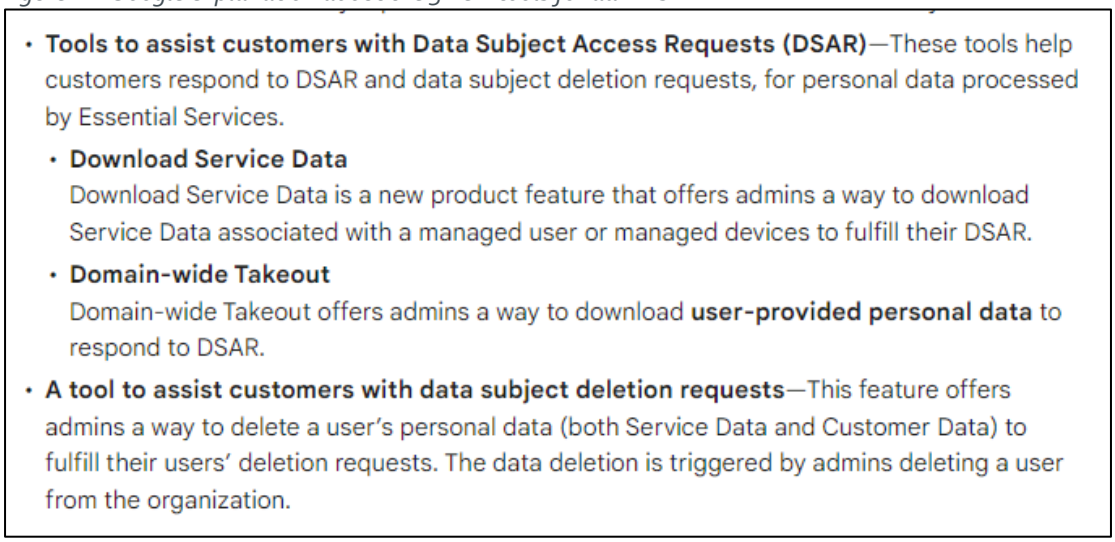
2.1.1 Download Service Data

Figure 10: Data Subject Rights tools available for admins in the processor ChromeOS



All three hyperlinks under 'Learn more' and the hyperlinked text 'Learn more about data processor mode' lead to the same Chrome Help Article: '*ChromeOS data processor mode—Overview for schools*'.[26] This article contains a very brief explanation about the three tools, as shown in Figure 11 below.

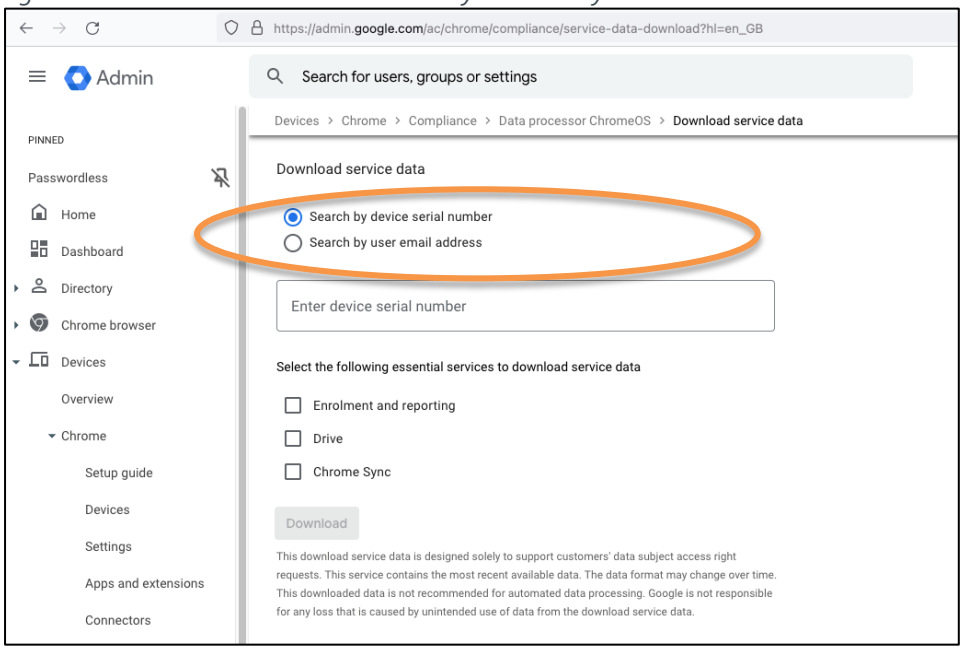
Figure 11: Google explanation about the 3 new tools for admins[27]



[26] Chrome Help article, Overview of ChromeOS data processor mode, undated, page last visited 21 February 2024, URL: https://support.google.com/chrome/a/answer/13605764 .
[27] Idem.

The first tool, Download Service Data, offers two options to admins: to query for the available Diagnostic Data relating to a specific Chromebook device, or to query for the Diagnostic Data relating to a specific student.

Figure 12: Download Service Data: search by device or by user



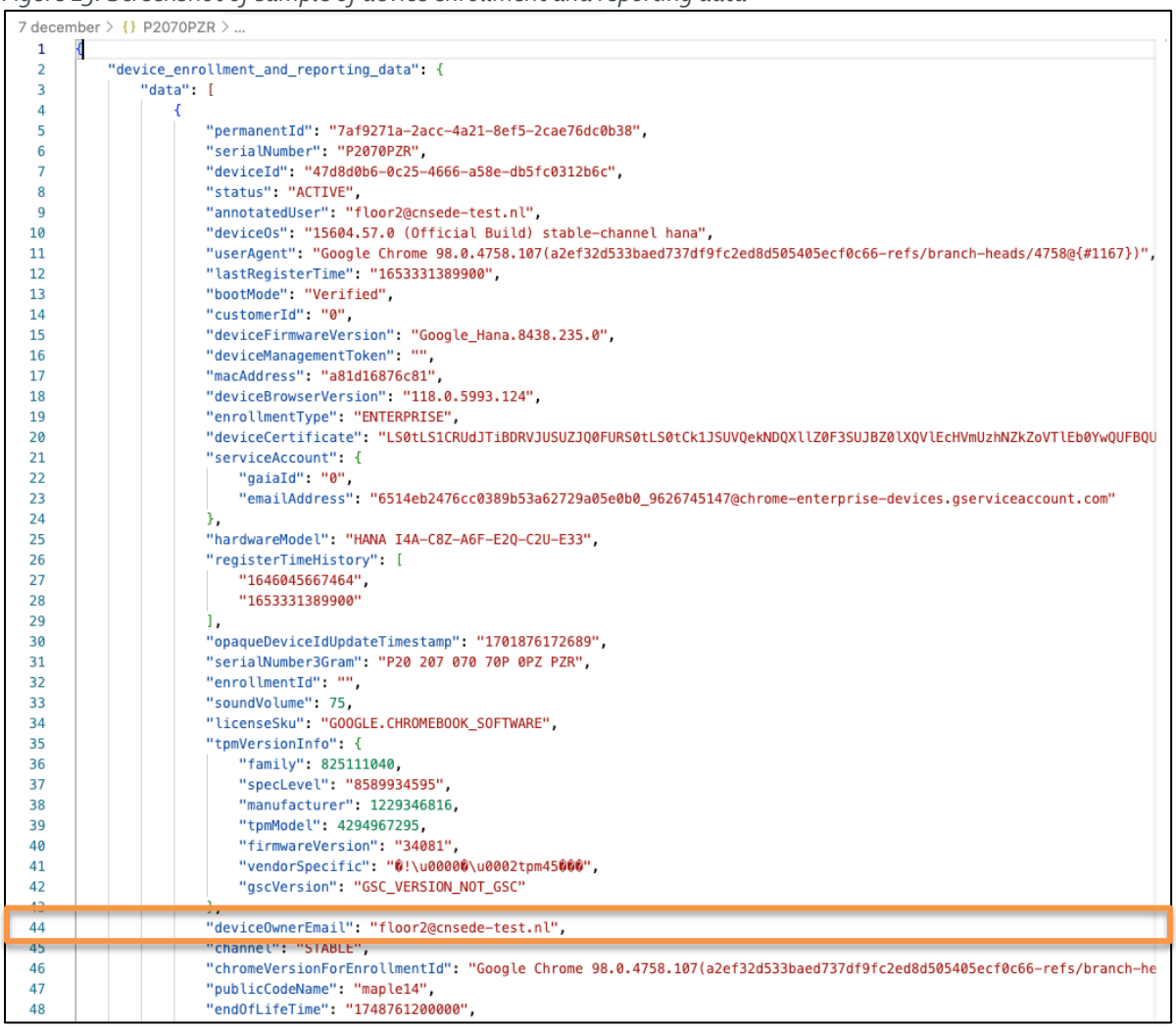
The outcomes of the two queries are different, and are separately described below.

Takeout Device serial number

If an admin executes the takeout option by device serial number, the admin receives a single file with a single category of data objects called 'device_enrollment_and_reporting_data'.

These data clearly identify the device owner through the e-mail address (see line 44 in Figure 13 below).The file also identifies other accounts that are active on the device. See Figure 14 below.

Figure 13: Screenshot of sample of device enrollment and reporting data[28]



7 december > {} P2070PZR > ...


```
{
    "device_enrollment_and_reporting_data": {
        "data": [
            {
                "permanentId": "7af9271a-2acc-4a21-8ef5-2cae76dc0b38",
                "serialNumber": "P2070PZR",
                "deviceId": "47d8d0b6-0c25-4666-a58e-db5fc0312b6c",
                "status": "ACTIVE",
                "annotatedUser": "floor2@cnsede-test.nl",
                "deviceOs": "15604.57.0 (Official Build) stable-channel hana",
                "userAgent": "Google Chrome 98.0.4758.107(a2ef32d533baed737df9fc2ed8d505405ecf0c66-refs/branch-heads/4758@{#1167})",
                "lastRegisterTime": "1653331389900",
                "bootMode": "Verified",
                "customerId": "0",
                "deviceFirmwareVersion": "Google_Hana.8438.235.0",
                "deviceManagementToken": "",
                "macAddress": "a81d16876c81",
                "deviceBrowserVersion": "118.0.5993.124",
                "enrollmentType": "ENTERPRISE",
                "deviceCertificate": "LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUVQekNDQXllZ0F3SUJBZ0lXQVlEcHVmUzhNZkZoVTlEb0YwQUFBQU
                "serviceAccount": {
                    "gaiaId": "0",
                    "emailAddress": "6514eb2476cc0389b53a62729a05e0b0_9626745147@chrome-enterprise-devices.gserviceaccount.com"
                },
                "hardwareModel": "HANA I4A-C8Z-A6F-E2Q-C2U-E33",
                "registerTimeHistory": [
                    "1646045667464",
                    "1653331389900"
                ],
                "opaqueDeviceIdUpdateTimestamp": "1701876172689",
                "serialNumber3Gram": "P20 207 070 70P 0PZ PZR",
                "enrollmentId": "",
                "soundVolume": 75,
                "licenseSku": "GOOGLE.CHROMEBOOK_SOFTWARE",
                "tpmVersionInfo": {
                    "family": 825111040,
                    "specLevel": "8589934595",
                    "manufacturer": 1229346816,
                    "tpmModel": 4294967295,
                    "firmwareVersion": "34081",
                    "vendorSpecific": "\u0000\u0000\u0002tpm45\u0000\u0000",
                    "gscVersion": "GSC_VERSION_NOT_GSC"
                },
                "deviceOwnerEmail": "floor2@cnsede-test.nl",
                "channel": "STABLE",
                "chromeVersionForEnrollmentId": "Google Chrome 98.0.4758.107(a2ef32d533baed737df9fc2ed8d505405ecf0c66-refs/branch-he
                "publicCodeName": "maple14",
                "endOfLifeTime": "1748761200000",
```

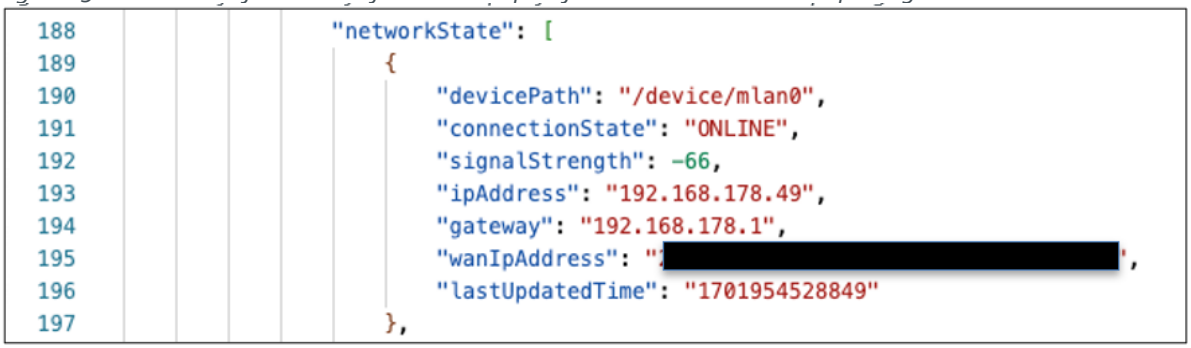

[28] Exported 7 December 2023, lay-out enhanced in Visual Studio Code.

Figure 14: Screenshot of more lines from the sample of device enrollment and reporting data [29]

```
137             "user": [
138                 {
139                     "type": "USER_TYPE_MANAGED",
140                     "email": "sjoera@cnsede-test.nl"
141                 },
142                 {
143                     "type": "USER_TYPE_MANAGED",
144                     "email": "floor@cnsede-test.nl"
145                 },
146                 {
147                     "type": "USER_TYPE_MANAGED",
148                     "email": "floor2@cnsede-test.nl"
149                 }
150             ],
```

The exported data also include device public and private network information.

Figure 15: Screenshot of more lines from the sample of device enrollment and reporting data [30]



```
188             "networkState": [
189                 {
190                     "devicePath": "/device/mlan0",
191                     "connectionState": "ONLINE",
192                     "signalStrength": -66,
193                     "ipAddress": "192.168.178.49",
194                     "gateway": "192.168.178.1",
195                     "wanIpAddress": "[redacted]",
196                     "lastUpdatedTime": "1701954528849"
197                 },
```

It is not clear how, in what structure and in what format, Google collects these *device_enrollment_ and_reporting_ data*. The bulk of data was clearly collected from the device, because it contains information generated on the device, such as, what user was using the specific device, or information about the device hardware. However, Privacy Company could not decrypt the intercepted Telemetry Data from the outgoing network traffic. Therefore, Privacy Company cannot conclude with certainty if this access in the Telemetry Data is complete.

On the other hand, no obviously generated information as a result of the tests is missing from these results.

[29] Exported 7 December 2023.
[30] Exported 7 December 2023. The IP address in line 195 has been masked on purpose.

Takeout e-mail address

If an admin executes the other takeout option, by e-mail address, the admin also receives a single file with json-data. This export contains four categories of data objects:

1. "user_enrollment_and_reporting_data"
2. "drive_client_service_data"
3. "drive_server_service_data"
4. "chromesync_service_data"

The first category '*user_enrollment_and_reporting_data'* clearly contains Telemetry events, as Google itself has named some events with the keyword Telemetry. These events are automatically sent from the ChromeOS to Google without any user action. The events in this category did not contain usernames or e-mail addresses. An example of a Telemetry event in this category is included in Figure 16 below, about the use of audio devices like a speaker or a headset. In a previous test, Google collected the name of Bluetooth earbuds in the telemetry events. During this test, the same named earbuds were used, but Google apparently no longer collects these identifying data.

Figure 16: Sample of a telemetry event about audio device usage


```
33          {
34              "key": "TelemetryTimeSeriesMetric",
35              "value": "TelemetryTimeSeriesMetric{customerId=0, metricEntityId=device_permanent_id:
                \"7af9271a-2acc-4a21-8ef5-2cae76dc0b38\"\nuser_gaia_id: 0\n, clientCollectedTime=2023-12-07T10:45:41.550Z,
                serverCollectedTime=2023-12-07T13:07:49.454478Z, audioTelemetry=Optional[audio_telemetry {\n  output_mute: false\n
                input_mute: false\n  output_volume: 100\n  output_device_name: \"Speaker\"\n  input_gain: 50\n  input_device_name:
                \"Internal Mic\"\n}\n], networksTelemetry=Optional.empty, userStatusTelemetry=Optional.empty,
                peripheralsTelemetry=Optional.empty, bootPerformanceTelemetry=Optional.empty, displaysTelemetry=Optional.empty,
                appTelemetry=Optional.empty, runtimeCountersTelemetry=Optional.empty}"
36          },
```


The Drive Client Service Data contains statistical information about the operation of the Google Drive Client application. Figure 17 below shows an example of the type of information collected from the Drive client on the Chromebook: the amount of time spent on various operations performed by the client, for example the time needed to access a file in storage. These events contain the IP address of the user in the metadata that go with the exported bundles.

Figure 17: Example of Drive Client Service Data event


```
147                 {
148                     "clientTimingInfo": {
149                         "elapsedTiming": {
150                             "endClientTimeUsec": "1701877703073447",
151                             "startClientTimeUsec": "1701877703073447"
152                         },
153                         "timingType": "ELAPSED"
154                     },
155                     "endSequenceNumber": "947",
156                     "eventCode": "79378",
157                     "highFrequencyDetails": {
158                         "closingTrigger": "THROTTLER_DELIVERY",
159                         "numActivityComponents": "1"
160                     },
161                     "startSequenceNumber": "946"
162                 },
```


The Drive Server Service Data did not contain any data. However, no test was performed with the storage of data in Drive for this Verification Report.

The fourth category of Chromesync_service_data contains a log of Chrome Sync activity. Figure 18 and Figure 19 below show examples of the data provided about the creation of a bookmark and the storing of a password in the password manager. The events only contain metadata, none of the contents (such as the URL or the password).

Figure 18: Example of recorded Sync event after creating a bookmark


```
11763         {
11764             "activityId": {
11765                 "timeUsec": "1701953641431000"
11766             },
11767             "actor": {
11768                 "email": "sjoera@cnsede-test.nl"
11769             },
11770             "event": [
11771                 {
11772                     "eventType": "generic_data_type",
11773                     "eventName": "add_data",
11774                     "parameter": [
11775                         {
11776                             "name": "data_type_name",
11777                             "value": "BOOKMARK",
11778                             "label": "LABEL_OPTIONAL",
11779                             "type": "TYPE_STRING"
11780                         }
11781                     ],
11782                     "eventId": "036495ef"
11783                 }
11784             ]
11785         },
```

Figure 19: Example of recorded Sync event after storing a password

```
11786       {
11787           "activityId": {
11788               "timeUsec": "1701879196020000"
11789           },
11790           "actor": {
11791               "email": "sjoera@cnsede-test.nl"
11792           },
11793           "event": [
11794               {
11795                   "eventType": "generic_data_type",
11796                   "eventName": "add_data",
11797                   "parameter": [
11798                       {
11799                           "name": "data_type_name",
11800                           "value": "PASSWORD",
11801                           "label": "LABEL_OPTIONAL",
11802                           "type": "TYPE_STRING"
11803                       }
11804                   ],
11805                   "eventId": "9f494816"
11806               }
11807           ]
11808       },
```

Google explains why it does not provide access to certain personal data in a help article called '*Additional information on data withheld for security purposes*'[31] 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.

Another reason to not provide access, is if the data are no longer available. Google has added some information about the retention periods of Chrome Diagnostic Data to a help article about the retention periods of Workspace data.[32]

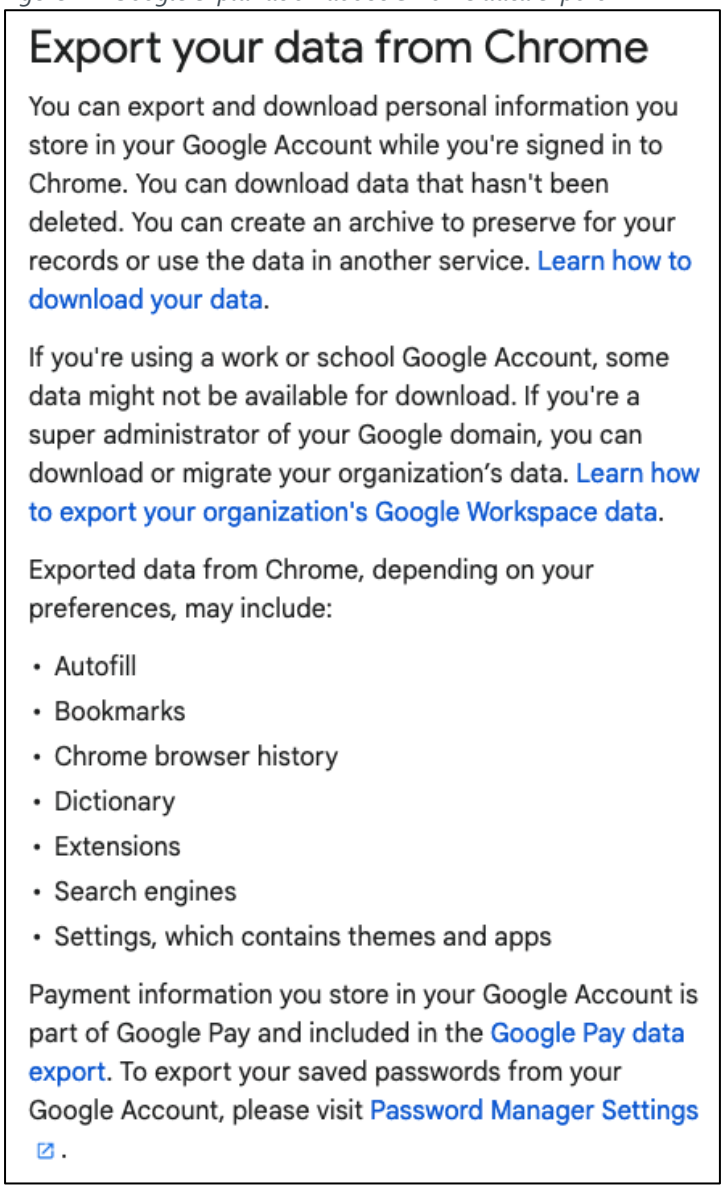
The results from the device and user takeout do contain some Telemetry Data, and reflect the test actions. However, due to the lack of detailed information about the Telemetry events, and the fact that Google withholds some information from DSAR results, it is difficult to verify the completeness of the personal data provided by Google.

[31] Google policies help, Information not provided in response to an access request, undated, page last visited 21 February 2024, URL: https://support.google.com/policies/answer/10972441.
[32] Google Workspace admin help, Data retention and lag times
Reports, security investigation tool, & audit and investigation page, undated, page last visited 21 February 2024, URL: https://support.google.com/a/answer/7061566?hl=en.

2.1.2 Takeout Customer Data

Google takeout for Chrome data is available for Chrome data and the configuration provided by the user. If an end-user goes to takeout.google.com, there is an option 'Chrome Data'. This contains a hyperlink to 'More info', and a further hyperlink 'See here for the type of data available for export.' This results in a pop-up with the explanation shown in Figure 20 below.

Figure 20: Google explanation about Chrome data export[33]



Export your data from Chrome

You can export and download personal information you store in your Google Account while you're signed in to Chrome. You can download data that hasn't been deleted. You can create an archive to preserve for your records or use the data in another service. Learn how to download your data.

If you're using a work or school Google Account, some data might not be available for download. If you're a super administrator of your Google domain, you can download or migrate your organization's data. Learn how to export your organization's Google Workspace data.

Exported data from Chrome, depending on your preferences, may include:

- Autofill
- Bookmarks
- Chrome browser history
- Dictionary
- Extensions
- Search engines
- Settings, which contains themes and apps

Payment information you store in your Google Account is part of Google Pay and included in the Google Pay data export. To export your saved passwords from your Google Account, please visit Password Manager Settings .

[33] Google, Export your data from Chrome, undated, page last visited 21 February 2024, URL: https://support.google.com/chrome/answer/10248834 .

Privacy Company filed an export request on 21 December 2023, in Google's general Customer Takeout form for admins in the Google Admin Console.[34] Even though Google warns that the admin needs to enable the Workspace Additional Service Google Cloud, in the test tenant Google Cloud Platform was disabled, as shown in Figure 21 below. However, Google did start the export. This is in line with Google's commitment that it would behave as data processor for this Chrome export tool.

Figure 21: Screenshot Workspace Additional Services in test tenant

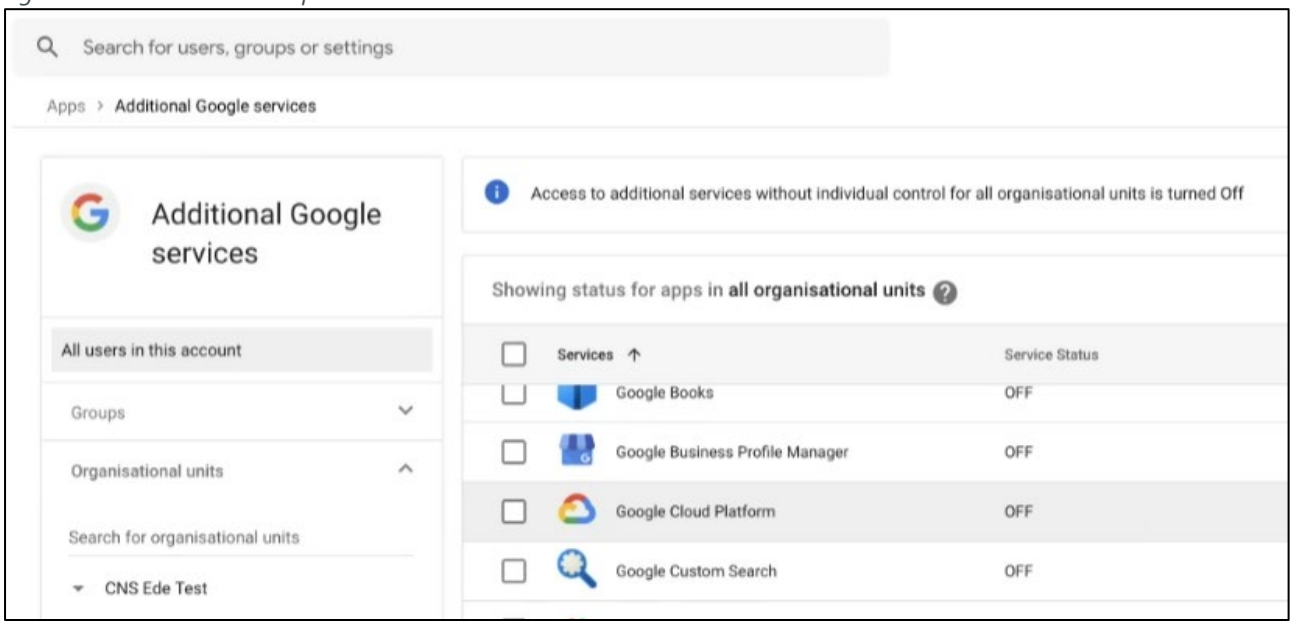
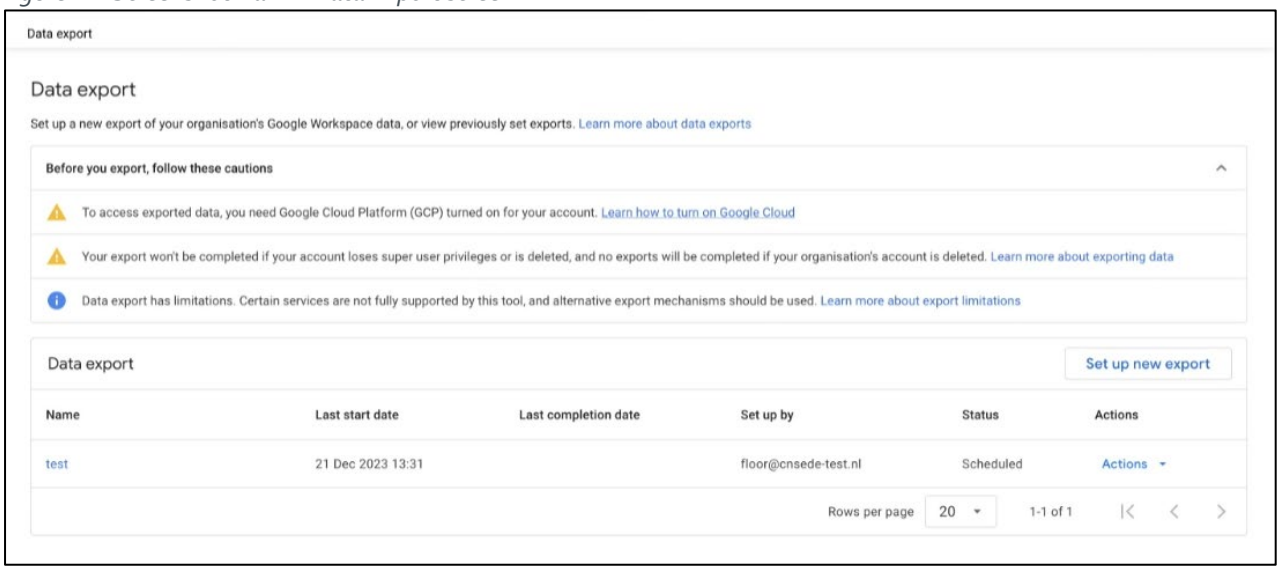
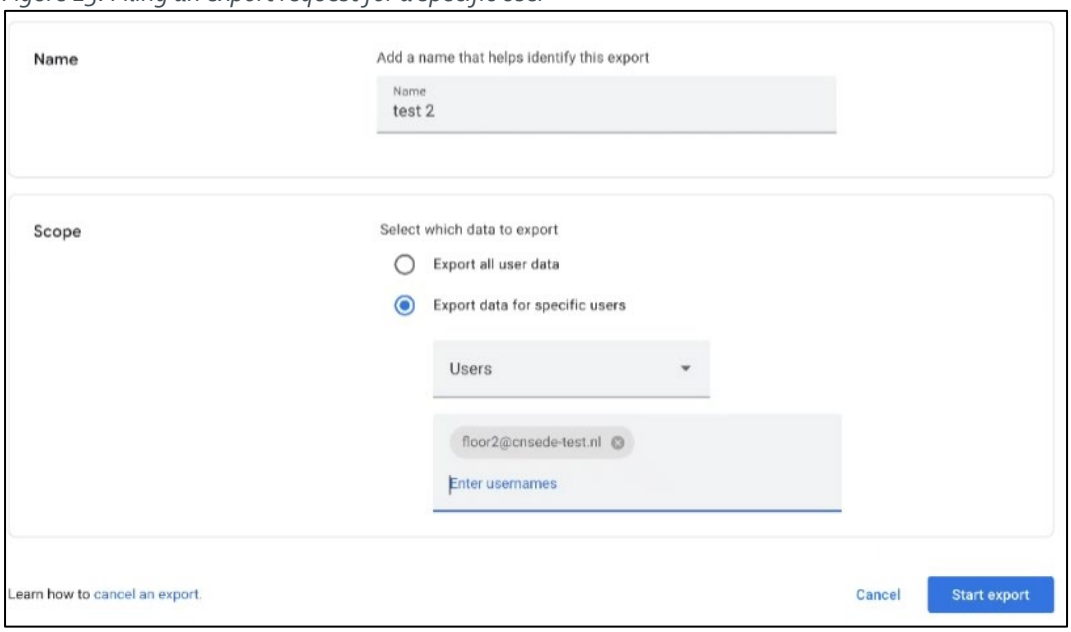


Figure 22: Screenshot Admin Data Export screen



[34] Google Admin Console Data Export Customer TakeOut, (access after log-in), URL: https://admin.google.com/ac/customertakeout

Figure 23: Filing an export request for a specific user



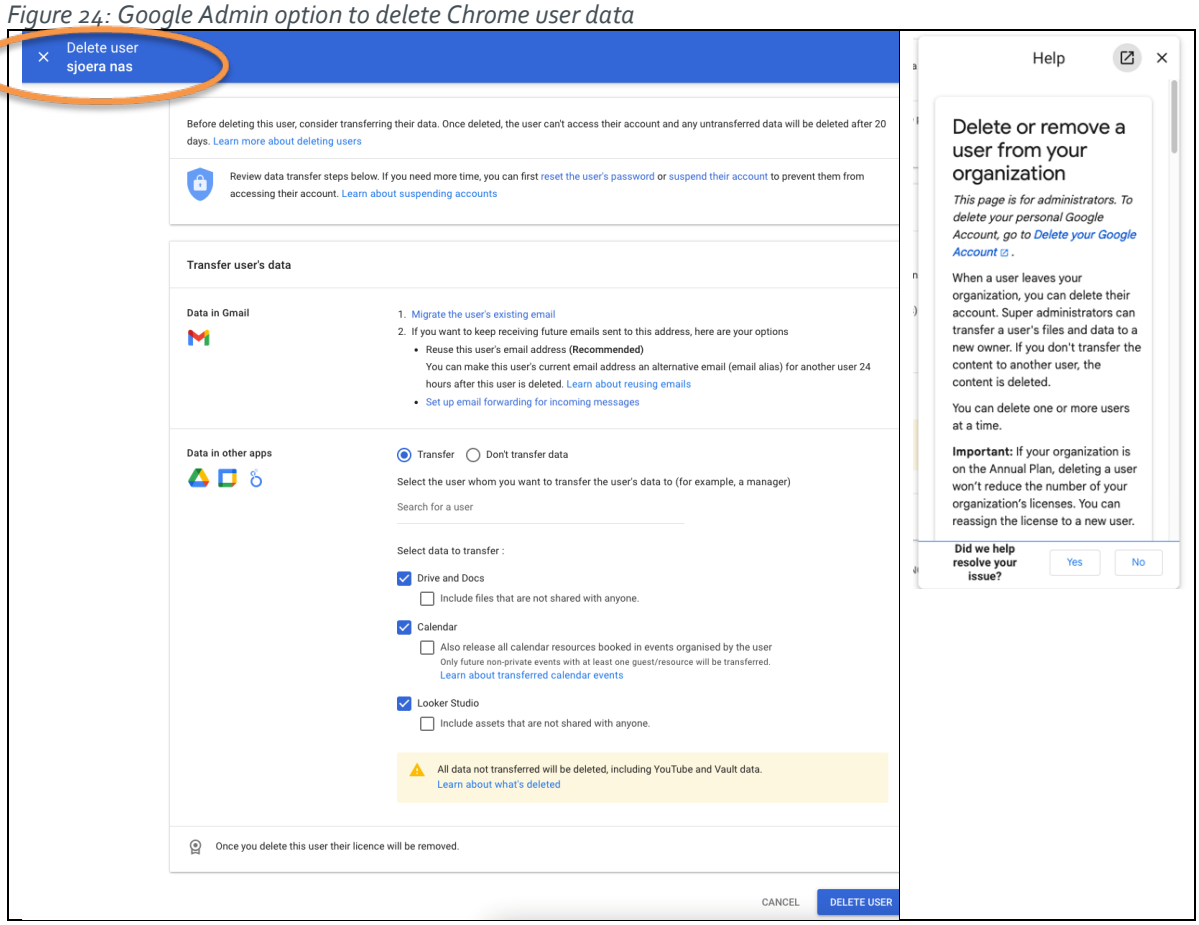
2.1.3 Delete user data

As show in Figure 24 below, Google created a new option in the Chrome processor category of the Google Admin Console to delete individual Google Account Data. Google warns admins that deletion takes place after 20 days, and offers an option to transfer Content Data to another account. Google also writes: "*All data not transferred will be deleted, including YouTube and Vault Data. Learn about what's deleted.*" The page contains a short help pop-up explaining the difference between transfer and deletion. The hyperlink at the bottom of the deletion page refers to a longer Help Article about the data that are deleted when an admin uses this option.[35]

The explanation does not contain any information about ChromeOS or Chrome browser data deletion, and does not mention the deletion of the Diagnostic Data (called Service Data by Google). However, after having deleted one of the test accounts in the test tenant, it was not possible anymore to download Service Data based on the deleted user's e-mail address. However, when downloading Service Data via the device serial number, the provided Service Data still contained references to the deleted user.

[35] Google, Delete or remove a user from your organization, undated, page last visited 21 February 2024, URL: https://support.google.com/a/answer/33314.

Figure 24: Google Admin option to delete Chrome user data



Via the hyperlink 'Learn about what's deleted' Google only provides information about deletion of Workspace Content Data. Google has not yet linked to its new Help article about Chrome data deletion. In that new Help Article Google explains what Chrome user data are deleted when an admin uses the new delete user function in the Chrome processor functionality in the Google Admin Console.[36] See Section 3.1 below.

In this new Chrome Help article Google explains that the Delete User tool enables administrators to search and delete a managed user's Personal Data, "*both Service Data and Customer Personal Data*." Google also explains this does not result in complete deletion: "*Note that not all Service Data is deleted through this process. Service Data processed by Essential Services for certain limited purposes (e.g., User Metrics) may be retained by Google and held for standard retention periods.*"

2.1.4 Workspace Telemetry viewer

Figure 25: Google's Diagnostic information tool [CONFIDENTIAL]

[36] Google, Chrome Enterprise and Education Help, Delete User Data, undated, page last visited 21 February 2024, URL: https://support.google.com/chrome/a/answer/13860429?hl=en&ref_topic=13844944&sjid=13183737250691098610-EU.

Google's Diagnostics Information Tool (DIT) is only available for Workspace services, not for Chrome, as shown in [CONFIDENTIAL] Figure 25 above. Google also does not provide a separate list of Chrome Telemetry events on its Workspace Telemetry information page (though Telemetry information is available elsewhere, in separate help articles).[37]

Google also offers a Telemetry Device API to admins.[38] With this access admins from managed Chrome devices can obtain device information for management purposes. Even though Google calls these data 'Telemetry Data' they are not identical to individual Telemetry events obtained from end user devices. Without a further explanation from Google, this source is out of scope of this verification report.

2.1.5 Overview available event logs

As shown in Table 2 below, Google also provides access to personal data to admins about the use of Chromebooks and the Chrome browser in different logs.

These are:

1. Admin log events
2. Device log events
3. Takeout log events
4. User log events

Previously, these logs were called audit logs, but Google has renamed them to log event data.[39] Google has published detailed information about the contents of these logs for admins[40] and the availability of event logs for security purposes.[41]

[37] Google Workspace Admin Help, Diagnostic Information Tool, undated, page last visited 21 February 2024, URL: https://support.google.com/a/answer/12830816
[38] Google, REST Resource: customers.telemetry.devices, undated, page last visited 21 February 2024, URL: https://developers.google.com/chrome/management/reference/rest/v1/customers.telemetry.devices
[39] Google Workspace Admin Help, undated, page last visited 21 February 2024, Improved audit and investigation experience, URL: https://support.google.com/a/answer/11339435 .
[40] Google, Run a search in the investigation tool, undated, URL last visited 21 December 2023, URL: https://support.google.com/a/topic/11479095.
[41] Google, Chrome log events, undated, last visited 21 February 2024, URL: https://support.google.com/a/answer/9393909

Table 2: Overview available personal data in admin logs[42]

Log name	Data available	In scope	Explanation
Access Transparency log events	No	No	N/A
Admin data action log events	No	No	N/A
Admin log events	Yes	Yes, may include status changes of Chromebooks	Contains a log of actions performed in the admin console, such as adding a user or changing ChromeOS settings.
Assignments log events	No	No	N/A
Calendar log events	No	No	N/A
Chat log events	No	No	N/A
Chrome log events[43]	No	Unknown, not yet available	Google published a new page about available log events for admins for security monitoring, but these data were not available when the tests for this report were performed[44]
Chrome Sync log events[45]	Yes	Yes	Contains Chrome Sync (bookmark, password manager, etc.) logs. No content data.
Classroom log events	No	No	N/A
Cloud Search log events	No	No	N/A
Contacts log events	No	No	N/A
Context-aware access log events	No	No	N/A
Device log events[46]	No	Yes	May contain data from ChromeOS security events, similar to Chrome Log events. However, during the tests no security events occurred that

[42] Google provides detailed explanations about all the admin event logs. In this retest Privacy Company checked the information about three logs: (1) Chrome log events—Events and attributes, (2) Device log events. Google Chrome log events – Events and attributes, URL: https://support.google.com/chrome/a/table/13465257 and (3) Chrome Sync log events. Google explains that the lengthy list of device log events is only available in Enterprise Plus and Education Plus licenses. "*Admins with Cloud Identity Premium, Enterprise Standard, and Education Standard will also have access to the investigation tool, but only for the following data sources: Chrome log events, Device log events, Oauth log events, Rules log events, User log events, and Voice log events.*" Google, Device log events, undated, page last visited 21 February 2024, URL: https://support.google.com/a/answer/11478791.

[43] Google Chrome log events – Events and attributes, undated, page last visited 21 February 2024, URL: https://support.google.com/chrome/a/table/13465257 .

[44] Google Workspace Admin Help, Chrome log events, undated, URL: https://support.google.com/a/answer/11478284. URL last visited 21 December 2023. None of the events described on this page were visible in the tests.

[45] Google Chrome Sync Log Events, URL: https://support.google.com/a/answer/12971803

[46] Google provides an exhaustive list of the events in this log at the URL: https://support.google.com/a/answer/11478791.

			were significant enough to trigger a logged event.[47]
Devices	Yes	Yes	Contains a list of devices use with the Google-accounts, including ChromeOS devices.
Directory Sync log events	No	No	N/A
Drive log events	Yes	No	N/A
Gmail log events	Yes	No	N/A
Gmail messages		No	N/A
Graduation log events	No	No	N/A
Groups enterprise log events	No	No	N/A
Groups log events	No	No	N/A
Keep log events	No	No	N/A
LDAP log events	No	No	N/A
Looker Studio log	No	No	N/A
Meet log events	Yes	No	N/A
OAuth log events	Yes	No	N/A
Password Vault log events	No	No	N/A
Profile log events	No	No	N/A
Rule log events	No	No	N/A
SAML log events	No	No	N/A
Takeout log events	Yes	Yes, if a user attempts to takeout Chrome data	N/A
Tasks log events	No	No	N/A
User log events[48]	Yes	Yes	N/A
Users	Yes	Yes	Contains basic metadata about all user accounts (last login, admin status, etc.)
Vault log events	No	No	N/A

The initial Chrome verification report includes examples from the different logs with personal data about interactions with the Chromebook and the Chrome browser. These examples are not repeated here. Google has made new logs available since June 2023. These are included in the table above.

[47] Google, Device log events, Security investigation tool, undated, page last visited 21 February 2024, URL: https://support.google.com/a/answer/11478791?hl=en.

[48] This is Google's new name for the combined old Login and User accounts audit logs.

2.2 Assessment

Google has developed three new features to help customers fulfil the data subject rights' requests they receive in their role as data controllers. These are assessed below.

2.2.1 Download Service Data

The two options to download Service Data function as expected. Privacy Company cannot conclude with certainty if the Telemetry Data are complete in the Takeout via e-mail address, but no obviously generated information as a result of the tests is missing from these results. The Takeout via device identifier does provide access to some Telemetry events, as Google itself has named some events with the keyword Telemetry. The events in this category did not contain user names or e-mail addresses. The category of Chrome Sync data does contain user identifiers, but does not contain the contents of synced passwords or bookmarks. In sum, the Service Data download option works as expected, without any excessive or obviously missing data.

2.2.2 Takeout Customer Data

It follows from the test performed by Privacy Company in the K-12 test tenant that admins do not need to enable a Google controller service for the individual export of Content Data from end users. Google has hence fulfilled its commitment to develop this processor service.

2.2.3 Delete User Data

The new option to delete user data seems only partially effective. In spite of Google's claim that the deletion tool would delete both Chrome Content and Service Data, it is not possible to delete ChromeOS and Chrome browser Diagnostic Data. When Privacy Company downloaded Service Data via the device serial number after account deletion, the provided Service Data still contained references to the deleted user. It is unclear if these data belong to the category of user metrics that Google says it retains longer. However, according to Google's table with information about the contents of different logs, these data should not contain any personal data, and hence, should not surface when a device-keyed query is performed.

The tool only deletes a Google user account, and the Content Data created or received by users with their account, such as e-mail, documents in Drive and (web)Pages. Google does not explicitly mention it will delete the Chrome Sync Content Data on account deletion, and it was not possible to verify deletion after account deletion.

2.2.4 Telemetry Viewer

Google did not expand its Diagnostic Information Tool to view the Telemetry Data from ChromeOS and Chrome browser.

2.2.5 Available event logs for admins

The event logs for admins provide adequate access to the data needed for admins to manage the managed Chrome environment, for example for security and update purposes. Admins can query the event logs to retrieve additional personal data from an individual end user in reply to a Data Subject Access Request, to complement the data provided by Google via the new Chrome processor Service Data Download tool.

2.2.6 Google explanation about information not provided in reply to DSAR

Google has improved its public information about reasons to refuse access to some personal data. Google has published a detailed explanation about reasons to refuse access for all of its services.[49] These explanations are convincing.

These reasons include:

1. Information relating to someone else
2. Anonymised data
3. Data Google cannot reliably relate to the requesting data subject
4. Data that could be used to undermine the security of Google's systems
5. Data that could infringe on the rights and freedoms of others (for example, legal privilege)[50]

The reasons Google does not provide separate access to logged data about cookies is that Google maintains it cannot reliably identify the person behind a cookie.

Google explains in its Privacy Help Center: "*A user's knowledge or possession of information (e.g. forwarded emails, details of IP addresses from which an account was accessed or cookie IDs), taken alone, is generally insufficient to verify that the user making a request is the individual to whom such data relates.*
For example, emails, IP addresses or device information could be obtained by third parties through various means, such as a spouse/partner that shares a device or gains access to an account of their partner forwarding emails to themselves which they subsequently submit in order to hijack an account. Similarly, third parties could alter the contents of automated emails so that they appear to relate to a different account. Similarly, IP addresses and cookie ID, taken alone, are generally inadequate for verification purposes for many reasons, including because they can be shared by a number of different people at the same time."[51]

---

[49] Google, Information not provided in response to an access request, undated, page last visited 21 February 2024, URL: https://support.google.com/policies/answer/10972441.
[50] Idem.
[51] Google Privacy Help Center, undated, page last visited 21 February 2024, URL: https://support.google.com/policies/answer/9581826?hl=en, under Verifying the identity of the individual making a request', third paragraph: 'Can I use other information related to or from a Google account to access data associated with that Google account?'

With regard to the Security Data Google processes as data controller, Google explains that it does not categorically refuse access to personal data that are used in security logs, as many of these data, such as device fingerprints and IP addresses are available in other copies of the data, used for other purposes. Google only refuses to provide access to what it calls "*sensitive configuration details, commercially sensitive indications of our approach to backup and archiving, and, most importantly, embodies architectural information about our approach to defense-in-depth.*"[52]

Google explains: "*If certain detailed information, about our system defenses, and the data we process through them, such as how low-level data structures are laid out in memory, were to become , it could give potential bad actors valuable signals that could be used to exploit our systems*."[53]

Privacy Company assesses these explanations as convincing. As established in the Update DPIA report, it is up to the supervisory authority, the Dutch Data Protection Authority, to assess whether a school (in its future role as data controller for the Essential ChromeOS and browser services) complies with the requirements of the GDPR in reply to data subject access requests, if a user complains that the access would be insufficient.

[52] Google, Information not provided in response to an access request.
[53] Idem.

3. Google documentation

This section answers the third question:

Does Google's public documentation about the data types collected by the Chrome processor OS and browser enable schools to adequately inform end-users??

3.1 Findings

Google has published three new Help Articles with documentation about the personal data it processes in Chrome processor mode: about the Chrome Essential Services, and about the Chrome data that are deleted when an admin deletes a user.

The first publication contains an explanation about the new Download Service Data option.[54] The article contains a table with a list of Essential Services, and if the data from that service are provided through the tool, or not. The list does not contain hyperlinks leading to more detailed information about the provided data.

Table 3: Google documentation of personal data provided through Chrome Download Service Data[55]

Essential Services	Covered by the tool	Notes
Enrollment / Device Verification	Y	None
Policy Management	N	This service does not process Personal Data
User & Device Reporting	Y	None
Kiosk Mode	N	This service does not process Personal Data
Managed Guest Sessions	N	This service does not process Personal Data
Google Drive Syncing	Y	None
Location Services	N	Personal data processed by this service is not directly tied to authenticated users or identifiable devices
Time Services	N	Personal data processed by this service is not directly tied to authenticated users or identifiable devices
Quick Answers - Translation	N	This service does not process Personal Data
Chromebook Recovery Utility	N	This service does not process Personal Data
Screencast	N	This service does not process Service Data, only Customer Personal Data
Spell Check (Basic)	N	This service does not process Personal Data
Enhanced Spell Check	N	This service does not process Personal Data

[54] Google, Download Service Data, undated, page last visited 21 February 2024, URL: https://support.google.com/chrome/a/answer/13843530.
[55] Idem.

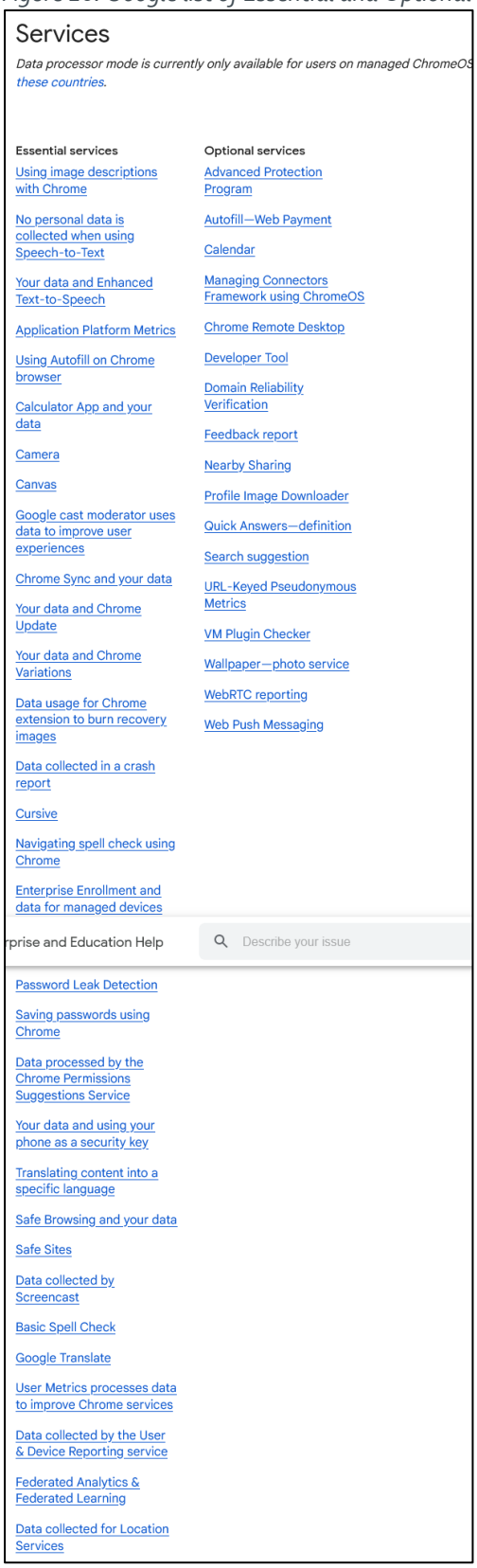
Application Platform Metrics	N	Personal Data processed by this service is pseudonymized and not tied to an identifiable individual or device
Calculator	N	Personal Data processed by this service is pseudonymized and not tied to an identifiable individual or device
Camera app	N	Personal Data processed by this service is pseudonymized and not tied to an identifiable individual or device
Canvas app	N	This service does not process Service Data
Cursive app	N	This service does not process Service Data
Files app	Y	For relevant data handled by Google Drive Syncing
Translate	N	This service does not process Personal Data
Chrome Sync	Y	None
Safe Browsing	N	Personal Data processed by this service is pseudonymized and not tied to an identifiable individual or device
Safe Sites	N	Personal Data processed by this service is pseudonymized and not tied to an identifiable individual or device
Autofill (excluding payment information)	Y	For relevant data handled by Chrome Sync
Phone-as-a-Security-Key	N	This service does not process Personal Data
Password Manager	Y	For relevant data handled by Chrome Sync
Permission Suggestions	N	Personal data processed by this service is not directly tied to authenticated users or identifiable devices
Chrome Update	N	Personal Data processed by this service is pseudonymized and not tied to an identifiable individual or device
Chrome Variations	N	This service does not process Personal Data
User Metrics	N	Personal Data processed by this service is pseudonymized and not tied to an identifiable individual or device
Crash Report	N	Personal Data processed by this service is pseudonymized and not tied to an identifiable individual or device
Cast Moderator	N	Personal Data processed by this service is pseudonymized and not tied to an identifiable individual or device
Accessibility—Speech-to-Text	N	This service does not process Personal Data
Accessibility—Text-to-Speech	N	This service does not process Personal Data
Accessibility—Image Annotation	N	This service does not process Personal Data

The second new Help Article contains a list of Essential and Optional Services with a hyperlink for each service to a short Help Article with a description of the data collection.[56] See Figure 26: Google list of Essential and Optional Services with hyperlinks

The linked article to for example Chrome Sync contains a table with a list of personal data. This list is descriptive, but not exhaustive. See Google for example writes it collects: "*Browser ID, Browser version & settings, Interaction of browser with Google products & services, Browser metrics and state.*" Google does not provide examples, so it remains unclear what 'Browser metrics' are, or to what level of detail Google collects 'Browser settings'. See Figure 26 below.

[56] Google Chrome Education and Enterprise Help, (List of Essential and Optional Chrome) Services, undated, page last visited 21 February 2024, URL: https://support.google.com/chrome/a/topic/13597460.

Figure 26: Google list of Essential and Optional Services with hyperlinks



Services

Data processor mode is currently only available for users on managed ChromeOS these countries.

Essential services

Using image descriptions with Chrome

No personal data is collected when using Speech-to-Text

Your data and Enhanced Text-to-Speech

Application Platform Metrics

Using Autofill on Chrome browser

Calculator App and your data

Camera

Canvas

Google cast moderator uses data to improve user experiences

Chrome Sync and your data

Your data and Chrome Update

Your data and Chrome Variations

Data usage for Chrome extension to burn recovery images

Data collected in a crash report

Cursive

Navigating spell check using Chrome

Enterprise Enrollment and data for managed devices

Optional services

Advanced Protection Program

Autofill—Web Payment

Calendar

Managing Connectors Framework using ChromeOS

Chrome Remote Desktop

Developer Tool

Domain Reliability Verification

Feedback report

Nearby Sharing

Profile Image Downloader

Quick Answers—definition

Search suggestion

URL-Keyed Pseudonymous Metrics

VM Plugin Checker

Wallpaper—photo service

WebRTC reporting

Web Push Messaging

rprise and Education Help

Describe your issue

Password Leak Detection

Saving passwords using Chrome

Data processed by the Chrome Permissions Suggestions Service

Your data and using your phone as a security key

Translating content into a specific language

Safe Browsing and your data

Safe Sites

Data collected by Screencast

Basic Spell Check

Google Translate

User Metrics processes data to improve Chrome services

Data collected by the User & Device Reporting service

Federated Analytics & Federated Learning

Data collected for Location Services

Figure 27: Example of detailed description for Chrome Sync

Data processed by this service

Chrome Sync processes data to provide a seamless experience when using a profile across devices.

Data Type / Category	Description	Examples	Data Subject Rights supporting features
User created content	This is required to sync user profiles across devices.	Bookmark names, Autofill related information (excluding payment information)	Download Service Data, Takeout Customer Data, Delete User Data
User information	This is required to sync user profiles across devices.	User ID and metadata for user created content	Download Service Data, Takeout Customer Data, Delete User Data
Device information	This is required to recognize a device running a sync-enabled Chrome browser.	Device ID, manufacturer, model, OS type and version, device form factor	Download Service Data, Takeout Customer Data, Delete User Data
User usage information	This is required to sync users' interaction with Google products and services.	Details on how feature is used	Download Service Data, Takeout Customer Data, Delete User Data
Site information	This is required to sync users' interaction with Google products and services.	Browser history (not collected for Enterprise users)	Download Service Data, Takeout Customer Data, Delete User Data
Extension information	This is required to sync Chrome extension related information and settings.	Extension ID, extension type &amd; settings, extension metrics	—
Browser information	This is required to sync Chrome browser information.	Browser ID, Browser version & settings, Interaction of browser with Google products & services, Browser metrics and state	—

The third new Help Article contains a list of Chrome data that are deleted when an admin deletes a user.[57] See Table 4 below.

[57] Google Chrome Enterprise and Education Help, Delete User Data, undated, page last visited 21 February 2024, URL: https://support.google.com/chrome/a/answer/1386029?hl=en&ref_topic=13844944&.

Based on Googles explanatory notes in the third column of both tables, the most important reason for Google not to provide access is when the data are not directly tied to an identifiable device, or to an authenticated user. The other reason not to provide access through the tool is because the service does not process any personal data at all, according to Google.

Table 4: Google documentation of Chrome data deletion[58]

Essential Services	Covered by the tool	Notes
Enrollment / Device Verification	Y	None
Policy Management	N	This service does not process Personal Data
User & Device Reporting	Y	None
Kiosk Mode	N	This service does not process Personal Data
Managed Guest Sessions	N	This service does not process Personal Data
Google Drive Syncing	Y	None
Location Services	N	Personal data processed by this service is not directly tied to authenticated users or identifiable devices
Time Services	N	Personal data processed by this service is not directly tied to authenticated users or identifiable devices
Quick Answers - Translation	N	This service does not process Personal Data
Chromebook Recovery Utility	N	This service does not process Personal Data
Screencast	Y	This service does not process Service Data, only Customer Personal Data
Spell Check (Basic)	N	This service does not process Personal Data
Enhanced Spell Check	N	This service does not process Personal Data
Application Platform Metrics	N	Personal Data processed by this service is pseudonymized and not tied to an identifiable individual or device
Calculator	N	Personal Data processed by this service is pseudonymized and not tied to an identifiable individual or device
Camera app	N	Personal Data processed by this service is pseudonymized and not tied to an identifiable individual or device
Canvas app	Y	This service does not process Service Data
Cursive app	Y	This service does not process Service Data
Files app	Y	For relevant data handled by Google Drive Syncing.
Translate	N	This service does not process Personal Data
Chrome Sync	Y	None
Safe Browsing	N	Personal Data processed by this service is pseudonymized and not tied to an identifiable individual or device

[58] Idem.

Safe Sites	N	Personal Data processed by this service is pseudonymized and not tied to an identifiable individual or device
Autofill (excluding payment information)	Y	For relevant data handled by Chrome Sync
Phone-as-a-Security-Key	N	This service does not process Personal Data
Password Manager	Y	For relevant data handled by Chrome Sync
Permission Suggestions	N	Personal data processed by this service is not directly tied to authenticated users or identifiable devices
Chrome Update	N	Personal Data processed by this service is pseudonymized and not tied to an identifiable individual or device
Chrome Variations	N	This service does not process Personal Data
User Metrics	N	Personal Data processed by this service is pseudonymized and not tied to an identifiable individual or device
Crash Report	N	Personal Data processed by this service is pseudonymized and not tied to an identifiable individual or device
Cast Moderator	N	Personal Data processed by this service is pseudonymized and not tied to an identifiable individual or device
Accessibility—Speech-to-Text	N	This service does not process Personal Data
Accessibility—Text-to-Speech	N	This service does not process Personal Data
Accessibility—Image Annotation	N	This service does not process Personal Data

3.2 Assessment

As described in Section 2 above, the outputs of the Service Data tool are functional. To understand the output, Google committed to explain which data types are collected by each service, including diagnostic / telemetry data collected by these services to the extent they collect user or device associated data.

Google did publish new documentation. However, the explanation in the new Help Article about Chrome Download Service Data is limited to the list of Essential Services from which an admin could expect to see personal data. The article does not help the admins explain to students the full extent of personal data Google collects about their use of the Chromebook and browser, in particular through Telemetry.

Google has not published an integrated list of all Chrome Telemetry Data, or added these events to the existing documentation on Google Workspace Telemetry Events. Google makes the

information available in separate help articles. This scattered presentation makes it very difficult to compare the output from the Download Service Data tool with the executed test scenarios, and even more difficult to assess the legitimacy of the data collection. Because Telemetry Data collection is a dynamic process, and admins do not have an option to completely disable this data stream, to be in control admins would have do a daily comparison with their work tasks and the output from the device-keyed Service Data download.

Admins can add the results of a user query in the admin event logs to the output of a DSAR Request, and look up reasonably detailed documentation from Google per service (both for Essential and Optional Services). With the help of the overview from SIVON to guide admins to all Google's relevant sources of information[59], schools as data controllers should be able to comply with the transparency requirements of the GDPR in relation to the data it allows Google as processor to process.

[59] SIVON, source with all relevant Google information (in Dutch), URL https://sivon.nl/uitleg-transparantie-gegevensverwerkingen-google-workspace-for-education/

4. Effectivity of privacy settings in Chrome browser

This section answers the fourth question:

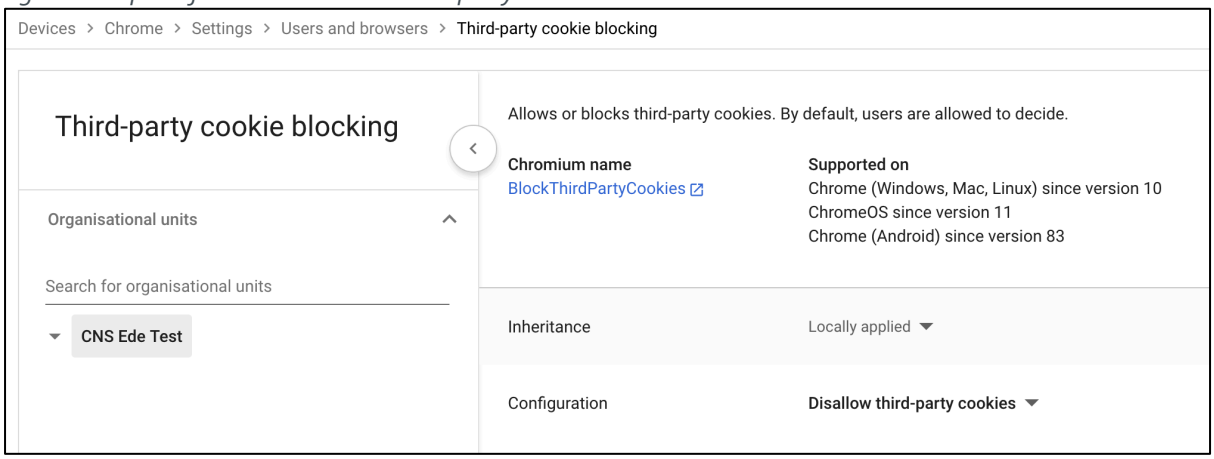
How effective are the privacy-friendly settings in the Chrome browser in blocking third-party cookies?

4.1 Findings

4.1.1 Third party cookies

Google allows admins to force the blocking of third party cookies on Chromebooks for logged-in users. Privacy Company reverified the effectiveness of this measure in the processor Chrome.

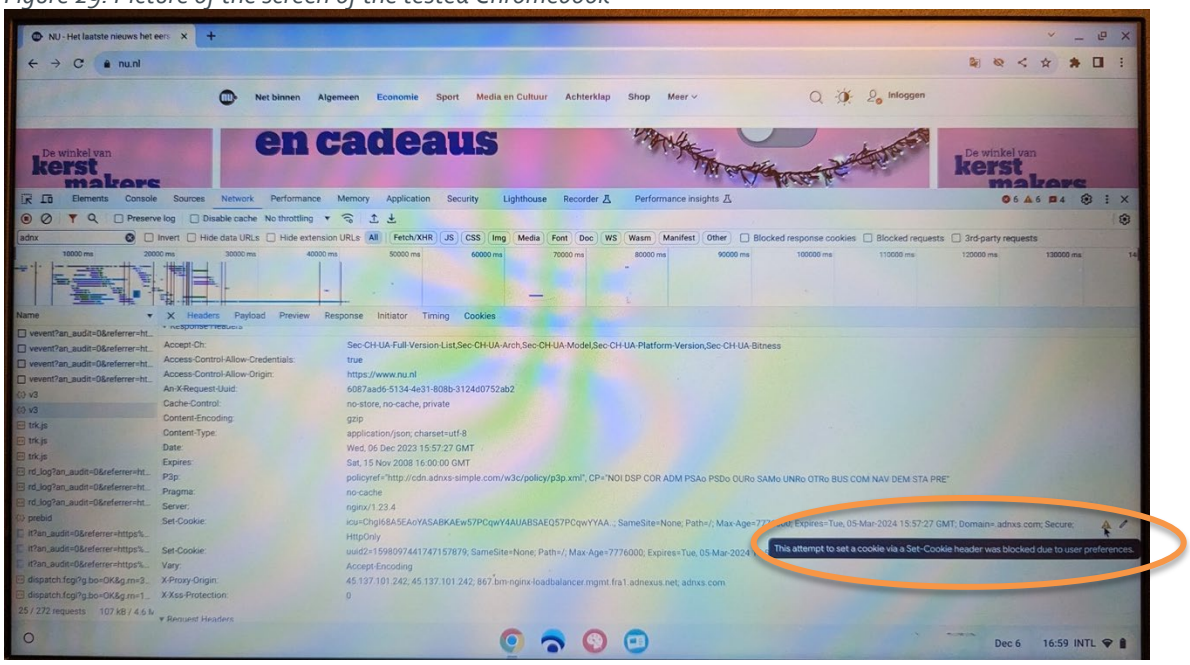
Figure 28: Option for admins to block third-party cookies



Privacy Company forced third-party cookie blocking in the admin console, and visited a large Dutch news website, nu.nl. This website contains many commercial ads. The website shows a consent pop-up for different types of cookies, but for the purposes of this test, all cookies were accepted.

As shown in Figure 29 below, the inspector mode of the browser showed a warning that the attempt to set a tracking cookie was blocked '*due to user preferences*'. This means that admins can effectively block tracking cookies, even when a user gives consent to a website to allow third party domains to set cookies for tracking purposes.

Figure 29: Picture of the screen of the tested Chromebook[60]



As mentioned in the first verification report, this tracking protection does not prevent exposure to first party advertising networks. Schools can mitigate this risk by centrally enforcing the Incognito mode to prevent such data leakage during a school day. Advertisers can use these data to profile students on the activities deployed that day, and use if for retargeting. If a student visits two websites with commercial advertisements, the second website may already contain ads for content shown on the first website, like shoes or bitcoins. Additionally, Internet tracking is more subtle than blocking third party cookies. Deleting tracking cookies does not help against other tracking technologies. Any party receiving a request can use the IP address, in combination with information about the browser and/or device configuration, to recognize a unique visitor.

4.1.2 Privacy Sandbox

Google uses the Privacy Sandbox as a tool to experiment with different privacy options. When tested, there were 3 options, all related to advertising:

Topics API[61]

This option enables Google to track an individual's web browsing history on the users' devices and generate a list of advertising "topics" based on the websites they visit. According to Google the most common topics are very coarse, such as "News", "Arts & Entertainment" and "Shopping".

[60] Picture taken from the Chromebook on 6 December 2023. It was not possible to capture the pop-up when making a screen capture on the device itself.

[61] See for an explanation in Dutch Tweakers, Google stopt met FLoC en stelt Topics-api voor als cookievervanging, 25 January 2022, URL: https://tweakers.net/nieuws/192438/google-stopt-met-floc-en-stelt-topics-api-voor-als-cookievervanging.html.

Google did not contradict a finding from the USA digital rights organisation EFF that in September 2023 there were almost 500 advertising categories—like "Student Loans & College Financing," "Parenting," or "Undergarments".[62] Google's Chrome team provided extra explanations about this functionality, but they are not relevant for this report. Advertising in the classroom is ethically undesirable, and personalised advertising is even more invasive. The Dutch education sector has signed a convenant with publishers of educational materials to prohibit advertising.

Site-suggested ads

This option allows advertisers to do what's called "remarketing" or "retargeting". This means if a user buys a product like a joystick online, many websites they visit later on will show them that same joystick. Disabling this functionality or the entire Privacy Sandbox does not mean users will not see advertisements on websites anymore: the Privacy Sandbox is not an ad blocker.

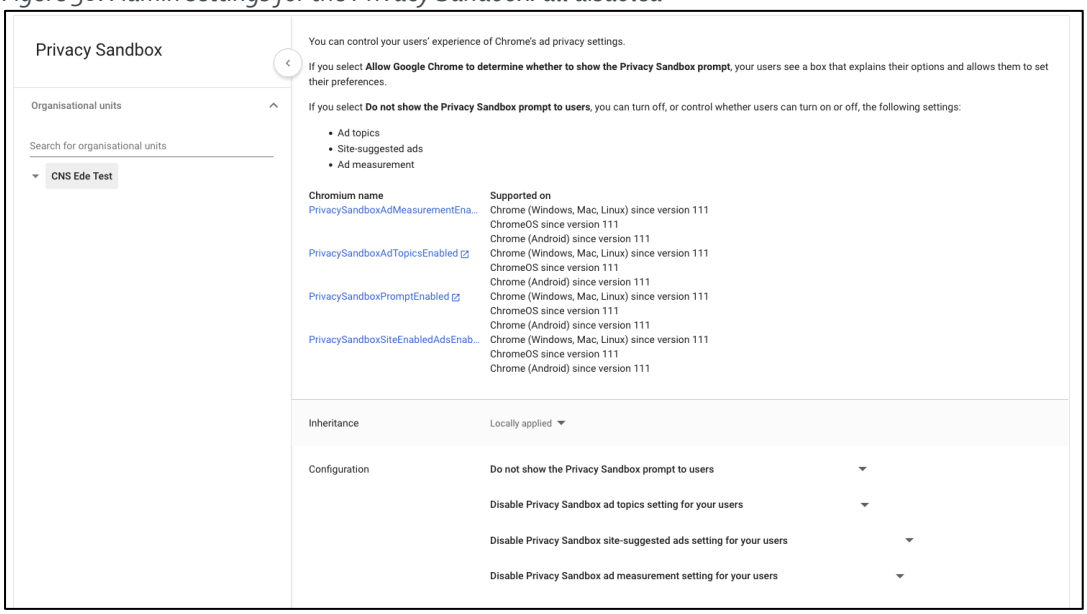
Ad measurement

This allows advertisers to track ad performance by storing conversion data in the users' browser that's then shared with the advertiser or advertising platform that the advertiser uses. For example, whether an ad click led to a conversion, on what website. The data that is stored and shared with the advertiser is limited to prevent cross site tracking of individual users through the use of noise, rate limits, and aggregation..

SIVON recommends to schools with existing managed Chromebooks to disable Privacy Sandbox completely. For new customers with a K-12 setting Google will disable Privacy Sandbox by default. As shown in Figure 30 in the test-tenant all 3 options were disabled.

[62] EFF, How To Turn Off Google's "Privacy Sandbox" Ad Tracking—and Why You Should, 28 September 2023, URL: https://www.eff.org/deeplinks/2023/09/how-turn-googles-privacy-sandbox-ad-tracking-and-why-you-should. The list of topics is available at https://github.com/patcg-individual-drafts/topics/blob/main/taxonomy_v2.md.

Figure 30: Admin settings for the Privacy Sandbox: all disabled



4.1.3 Do Not Track

Google does not offer an option to admins for the managed Chromebooks in processor mode to centrally enforce use of the Do Not Track signal in the browser. Google also does not offer another single central option to admins to block traffic to Google services where Google does not act as data processor (such as Analytics and Fonts). However, end users can enable DNT in their browser, and should be encouraged to do so by admins, and admins can use policies to restrict traffic through cookies and Javascripts from any third party, including Google.[63] [footnote to the two URLs].

4.1.4 Safe Browsing and Safe Sites

Google's functionality Safe Browsing protects users against suspicious URLs that may contain adult or explicit content. Though Google explains in the documentation about the data processing by Safe Browsing that "*Personal Data processed by this service is pseudonymized and not tied to an identifiable individual or device*", Google omits to explain it retains the end user IP addresses for a period of 7 days in case of a 'hit', a site with adult content. This was explained in the first Chrome verification report.[64] Admins can choose to allow standard Safe Browsing, or block this data processing completely. See Figure 31 and Figure 32 below. Googles 'Advanced' Safe browsing is an Optional (controller) Service.

[63] Chrome policies: https://chromeenterprise.google/policies/#JavaScriptBlockedForUrls and https://chromeenterprise.google/policies/#CookiesAllowedForUrls

[64] Privacy Company for SIVON, Inspection results Google Chrome for Education, 29 June 2023, p. 8, URL: https://sivon.nl/wp-content/uploads/2023/07/20230629-Chrome-inspection-report-v1-2-public-NEW.pdf.

Figure 31: Default settings and admin choices for Safe Browsing

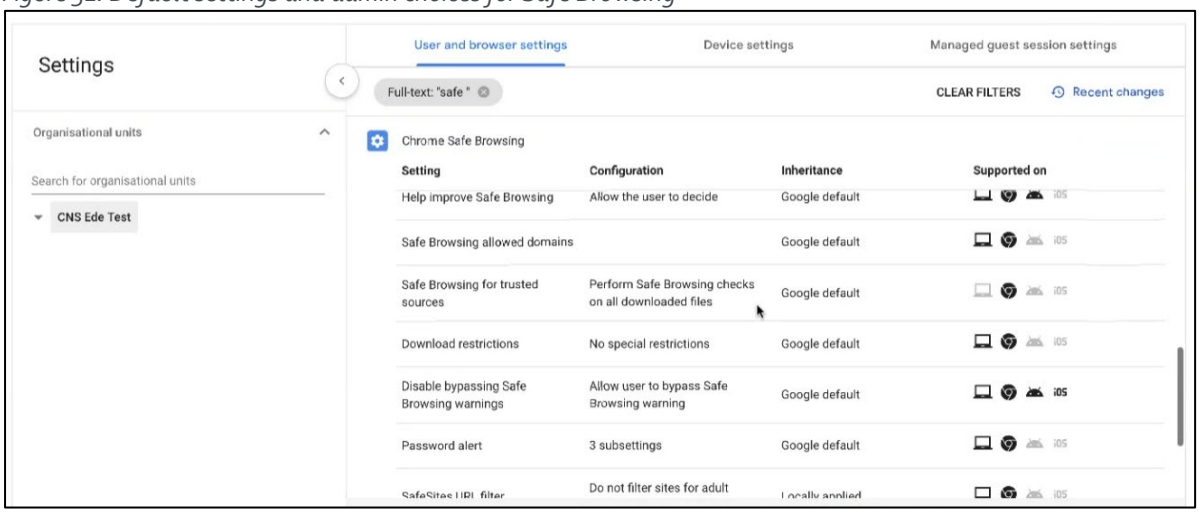
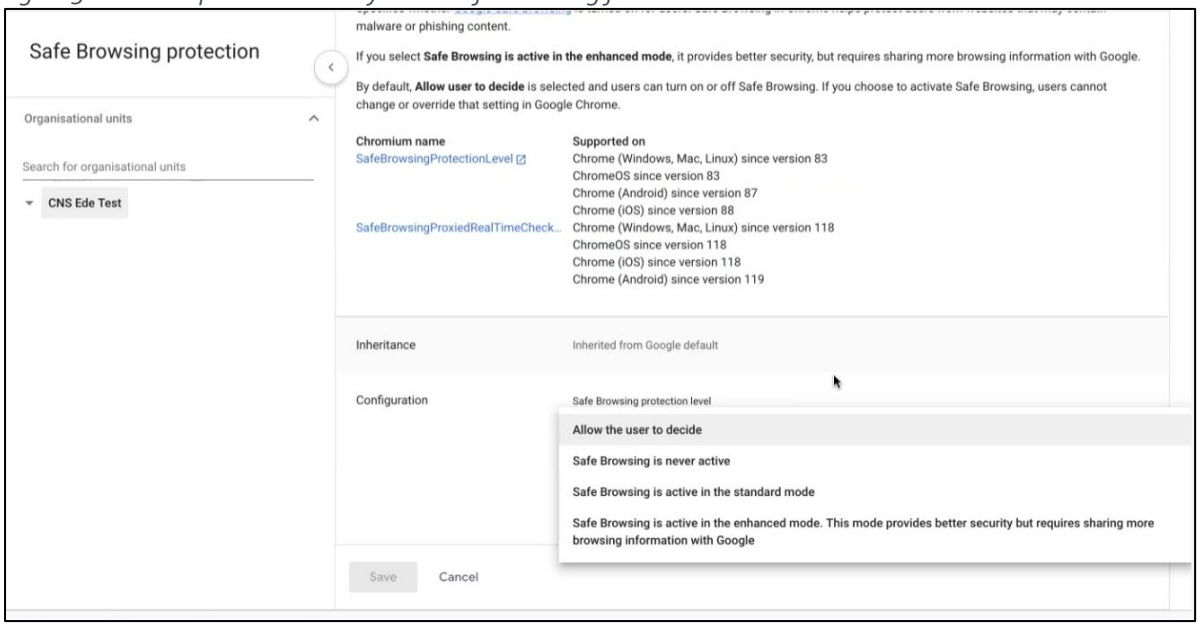


Figure 32: Admin option to centrally block Safe Browsing for all users



4.2 Assessment

Overall, the options for admins to block third party cookies, the Privacy Sandbox, Safe Browsing and Safe Sites seem reasonably effective in limiting the amount and contents of data transferred to third parties.

However, these options are not sufficient to prevent all forms of tracking. Chrome is effective in blocking third party cookies. There are high data protection risks related to personalised advertising, because of the inference of preferences based on surfing behaviour, the invisible *real time bidding* to show ads to people with specific profiles. The high risks relate to the lack of transparency of the data processing, in particular because of the unknown quantities of third

parties that may participate in the advertising space auctions, and the unknowable purposes for which they may further process the personal data. Because of these high risks, the European legislator has changed the opt-out requirement for tracking cookies to an opt-in requirement, back in 2009.[65]

The risks of profiling are even higher when it involves minors, due to their vulnerable nature. In the new EU Digital Services Act, providers of online platforms are prohibited from *presenting advertisements based on profiling using personal data of the recipient of the service when they are aware with reasonable certainty that the recipient of the service is a minor*.[66]

As explained in Section 4.1.1 blocking third party cookies does not offer complete protection against data leakage to advertising networks or against Google itself, in a role as data controller for *Additional Service*s such as Search and YouTube that can be visited by students, or use by websites of Google services such as analytics and fonts. And finally, tracking is not only based on cookies, but also on other data streams, such as the combination of an IP address with a unique browser and device configuration, and on URL parameters. These data streams may also involve transfers of personal data to third parties that use the data for advertising, and/or to third countries without an adequate data protection regime.

In sum, though Chrome is effective in blocking third party cookies, the browser does not offer protection against first party tracking, or against tracking by third party advertisers during a session, which may last a school day. Schools are advised to disable Safe Browsing and Safe Sites, or choose the least invasive 'Standard mode', and encourage students to enable the DNT signal in the Chrome browser. Schools can also choose to centrally enforce the Incognito mode to minimise data leakage during a school day.

[65] Citizens' Rights Directive 2009/136/EC, updating the ePrivacy Directive 2002/58. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0136&from=EN.
[66] EU Digital Services Act, consolidated text 15 July 2022, Recital 52b, URL: https://www.europarl.europa.eu/doceo/document/TA-9-2022-0269_EN.html#title2

5. Privacy-friendly settings managed Chromebooks for admins

This section answers the fifth question:

Can admins effectively block the Optional Services and web app store for which Google remains a data controller??

5.1 Findings

An *Essential Service* is a service that Google has determined is critical for ChromeOS or Chrome-on-ChromeOS to function correctly for Dutch public sector. All other services are classified as *Optional Services*. The list of Essential services is included in Appendix 1 in this report.

Google has agreed to develop switches for admins to control access to these services. By default Optional Services that process personal data are switched 'off'. Optional Services that do not process personal data are 'on' by default (but can be disabled).

Google explains: "*Existing customers migrating to the new data processor mode Terms of Service will retain their latest settings to avoid disruption, and can choose to leave on or turn off Optional Services as best suits their needs.*"[67]

[67] Google, ChromeOS data processor mode—Overview for enterprises, undated, page last visited 21 February 2024, URL: https://support.google.com/chrome/a/answer/13816756?hl=en

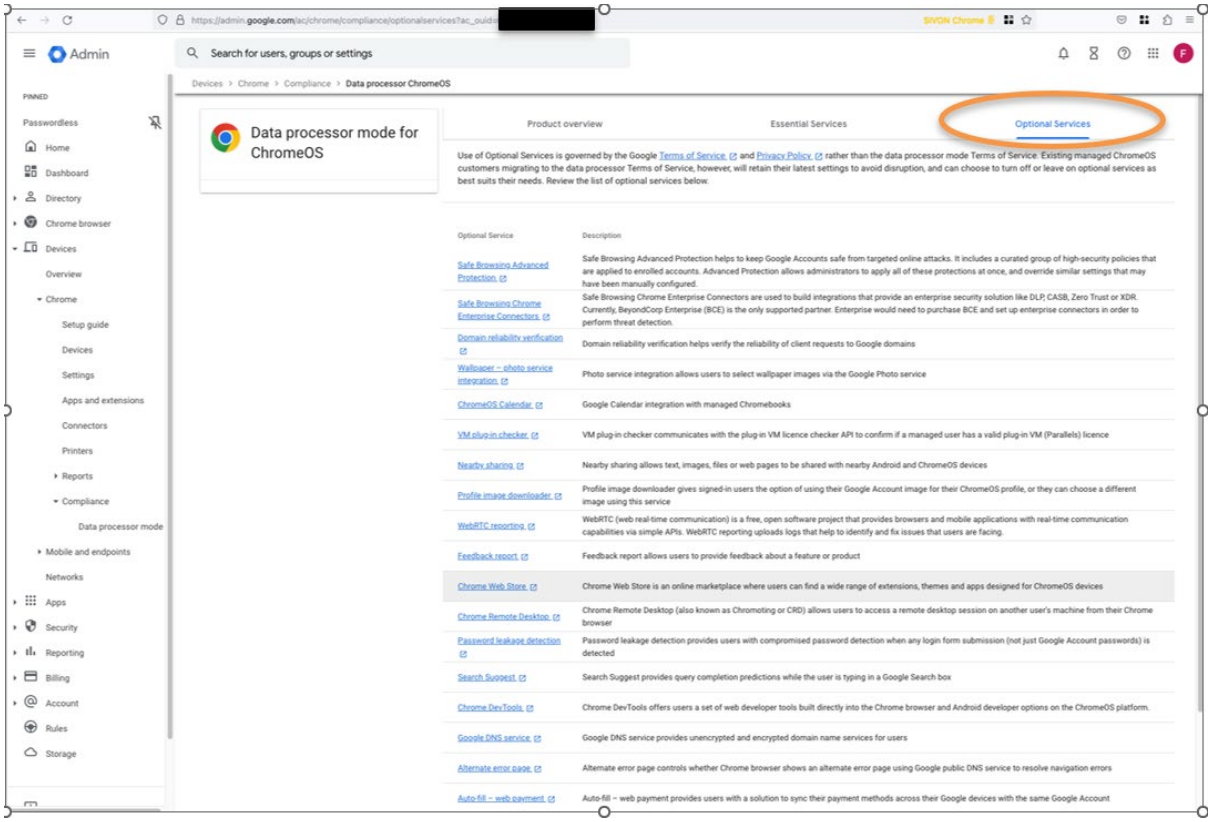


Table 5 below provides an overview of the switches Google makes available to admins to selectively enable or modify access to Optional services. Some settings allow the user of the device to overrule a setting chosen by the admin.

All of the Services in the first column contain a hyperlink to an action screen for the admin.

Table 5: Google overview of Optional Services that can be disabled by admins

Optional Service	Description
Safe Browsing Advanced Protection	Safe Browsing Advanced Protection helps to keep Google Accounts safe from targeted online attacks. It includes a curated group of high-security policies that are applied to enrolled accounts. Advanced Protection allows administrators to apply all of these protections at once, and override similar settings that may have been manually configured.
Safe Browsing Chrome Enterprise Connectors	Safe Browsing Chrome Enterprise Connectors are used to build integrations that provide an enterprise security solution like DLP, CASB, Zero Trust or XDR. Currently, BeyondCorp Enterprise (BCE) is the only supported partner. Enterprise would need to purchase BCE and set up enterprise connectors in order to perform threat detection.
Domain reliability verification	Domain reliability verification helps verify the reliability of client requests to Google domains

Optional Service	Description
Wallpaper – photo service integration	Photo service integration allows users to select wallpaper images via the Google Photo service
ChromeOS Calendar	Google Calendar integration with managed Chromebooks
VM plug-in checker	VM plug-in checker communicates with the plug-in VM licence checker API to confirm if a managed user has a valid plug-in VM (Parallels) licence
Nearby sharing	Nearby sharing allows text, images, files or web pages to be shared with nearby Android and ChromeOS devices
Profile image downloader	Profile image downloader gives signed-in users the option of using their Google Account image for their ChromeOS profile, or they can choose a different image using this service
WebRTC reporting	WebRTC (web real-time communication) is a free, open software project that provides browsers and mobile applications with real-time communication capabilities via simple APIs. WebRTC reporting uploads logs that help to identify and fix issues that users are facing.
Feedback report	Feedback report allows users to provide feedback about a feature or product
Chrome Web Store	Chrome Web Store is an online marketplace where users can find a wide range of extensions, themes and apps designed for ChromeOS devices
Chrome Remote Desktop	Chrome Remote Desktop (also known as Chromoting or CRD) allows users to access a remote desktop session on another user's machine from their Chrome browser
Password leakage detection	Password leakage detection provides users with compromised password detection when any login form submission (not just Google Account passwords) is detected
Search Suggest	Search Suggest provides query completion predictions while the user is typing in a Google Search box
Chrome DevTools	Chrome DevTools offers users a set of web developer tools built directly into the Chrome browser and Android developer options on the ChromeOS platform.
Google DNS service	Google DNS service provides unencrypted and encrypted domain name services for users
Alternate error page	Alternate error page controls whether Chrome browser shows an alternate error page using Google public DNS service to resolve navigation errors
Auto-fill – web payment	Auto-fill – web payment provides users with a solution to sync their payment methods across their Google devices with the same Google Account
URL-keyed pseudonymous metrics	URL-keyed pseudonymous metrics sends the URLs of pages that a user visits to Google to improve search and browsing.
Webpage messaging	Webpage messaging permits web pages to be sent push messages or notifications if a user has allowed Chrome notifications
Quick Answers – definition and unit conversion	Quick Answers definition and unit conversion features provide users with relevant results for the selected text.

5.2 Assessment

As a data controller for the managed Chrome and the Chromebooks, school admins can enforce privacy-friendly settings through the new Chrome Processor functionality in the Google Admin console.[68] These settings can be configured before providing the Chromebook to the student and can be changed remotely. The previous recommendations with regard to Optional Services are not repeated here. Schools are advised to follow the updated guidance from SIVON on the specific settings which privacy protective settings are still necessary to mitigate data protection risks[69].

[68] The admin console can be accessed through https://admin.google.com/ac/chrome/settings/[user?org=[unique id of the organisation]

[69] SIVON manual (in Dutch), URL: https://sivon.nl/wp-content/uploads/2023/09/Handleiding-ChromeOS-en-Chrome-browser.pdf

6. Use of managed Google Play Store

This section answers the sixth question:

Can schools use the managed Google Play store without data protection risks?

6.1 Findings

As discussed in the previous report, Google offers three different app stores:

1. Google Play, accessible from Android devices and Chromebooks, available in two flavours: general and *managed* Google Play
2. Chrome Web Store for the Chrome browser
3. Google Workspace Marketplace

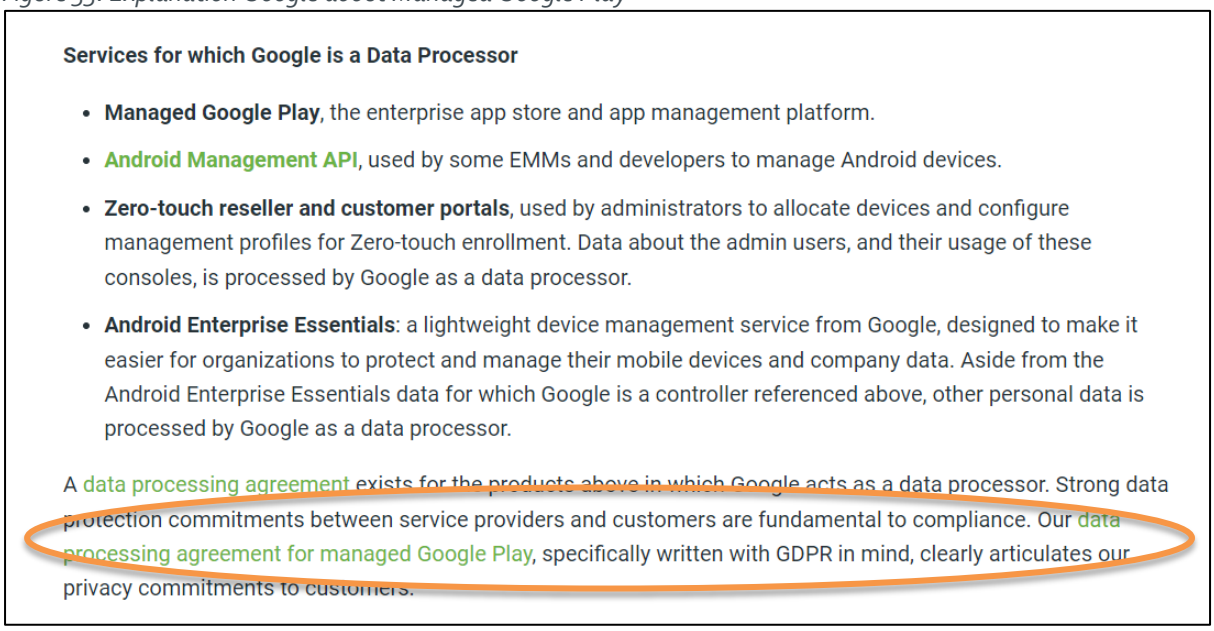
For this verification report, only access to the managed Google Play store was tested.
Google has not made any changes in its role as data controller for the Chrome Web Store and Google Play. Therefore the advice from the previous report is still valid that schools should block access to these services.

The previous report also concluded that the use of *managed* Google Play did not mitigate the data protection risks, since Google continued to act as data controller for the metadata (called Service Data by Google). Google confirmed: "*Google acts as a data processor for Managed Play for the customer data provided to Google in its provision of the services. Google is also a data controller for Google Play and for usage logs of users interacting with the Managed Play version of the store*."[70] Therefore, schools were advised to install apps for education through other methods, not through Google's app stores.

As shown in Figure 33 and Figure 34 below, Google did not change its legal terms for the *managed* Google Play store.

[70] Comment Google 22 February 2023.

Figure 33: Explanation Google about Managed Google Play[71]



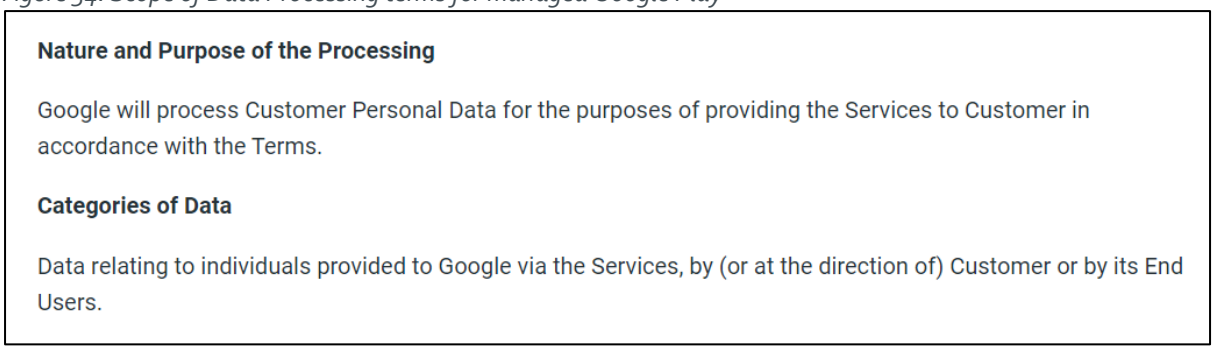
Services for which Google is a Data Processor

- **Managed Google Play**, the enterprise app store and app management platform.
- **Android Management API**, used by some EMMs and developers to manage Android devices.
- **Zero-touch reseller and customer portals**, used by administrators to allocate devices and configure management profiles for Zero-touch enrollment. Data about the admin users, and their usage of these consoles, is processed by Google as a data processor.
- **Android Enterprise Essentials**: a lightweight device management service from Google, designed to make it easier for organizations to protect and manage their mobile devices and company data. Aside from the Android Enterprise Essentials data for which Google is a controller referenced above, other personal data is processed by Google as a data processor.

A data processing agreement exists for the products above in which Google acts as a data processor. Strong data protection commitments between service providers and customers are fundamental to compliance. Our data processing agreement for managed Google Play, specifically written with GDPR in mind, clearly articulates our privacy commitments to customers.

The emphasised hyperlink in Figure 51 above leads to the Android Enterprise Data Processing and Security Terms.[72] These (recently updated) Android Data Processing and Security Terms only cover the limited category of 'Customer Data' in Managed Play.[73] That is: the Content Data actively provided by users, such as a review of an app, but not the Diagnostic Data (Service Data).

Figure 34: Scope of Data Processing terms for managed Google Play[74]



Nature and Purpose of the Processing

Google will process Customer Personal Data for the purposes of providing the Services to Customer in accordance with the Terms.

Categories of Data

Data relating to individuals provided to Google via the Services, by (or at the direction of) Customer or by its End Users.

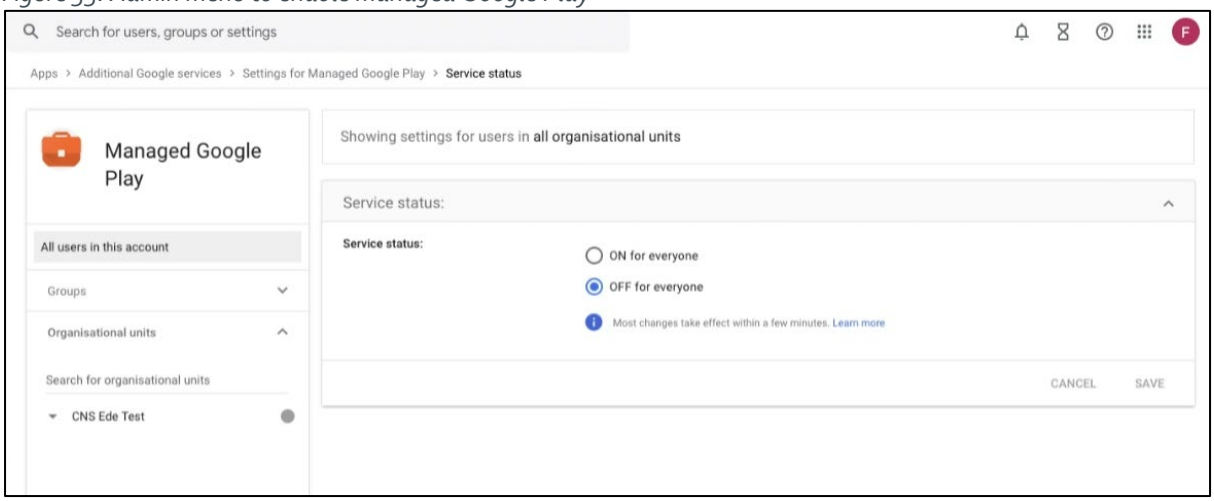
[71] Google, Android: our commitment to the GDPR for enterprise and education deployments, undated, page last visited 21 February 2024, URL: https://www.android.com/intl/nl_nl/enterprise/data-protection/

[72] Google, Managed Google Play Agreement, 23 March 2021, last visited 21 February 2024, URL: https://www.android.com/enterprise/terms/

[73] Android, Android Enterprise Data Processing and Security Terms, version November 2023, URL: https://www.android.com/enterprise/data-protection/terms In Article5.1.1 Google explicitly mentions the scope to Customer Personal Data: "*Google is a processor of that Customer Personal Data under the European Data Protection Legislation.*"

[74] Idem, Appendix 1: Subject Matter and Details of the Data Processing.

Figure 35: Admin menu to enable managed Google Play[75]



Managed Google Play remains a so called *Additional Service* in Google Workspace for Education. As shown in Figure 36 below, Google lists this service as an *Additional Service* in the Admin Console of the specific Workspace for Education tenant. Google therefore continues to act as data controller for these services.

When an admin wants to enable Managed Google Play, Google asks the admins to agree to the conditions that Google's general Privacy Policy applies, and that the school must have parental consent from any student under the age of 18.

Even if a school centrally blocks access to Google Play and to the managed Google Play, apps that are pushed by the school are still visible in the Google Play store. For this retest, Privacy Company force installed two apps: Squla and StudyGo.

[75] Screenshot made in the test tenant on 7 December 2023.

Figure 36: Admin Console listing Managed Google Play as Additional Service[76]

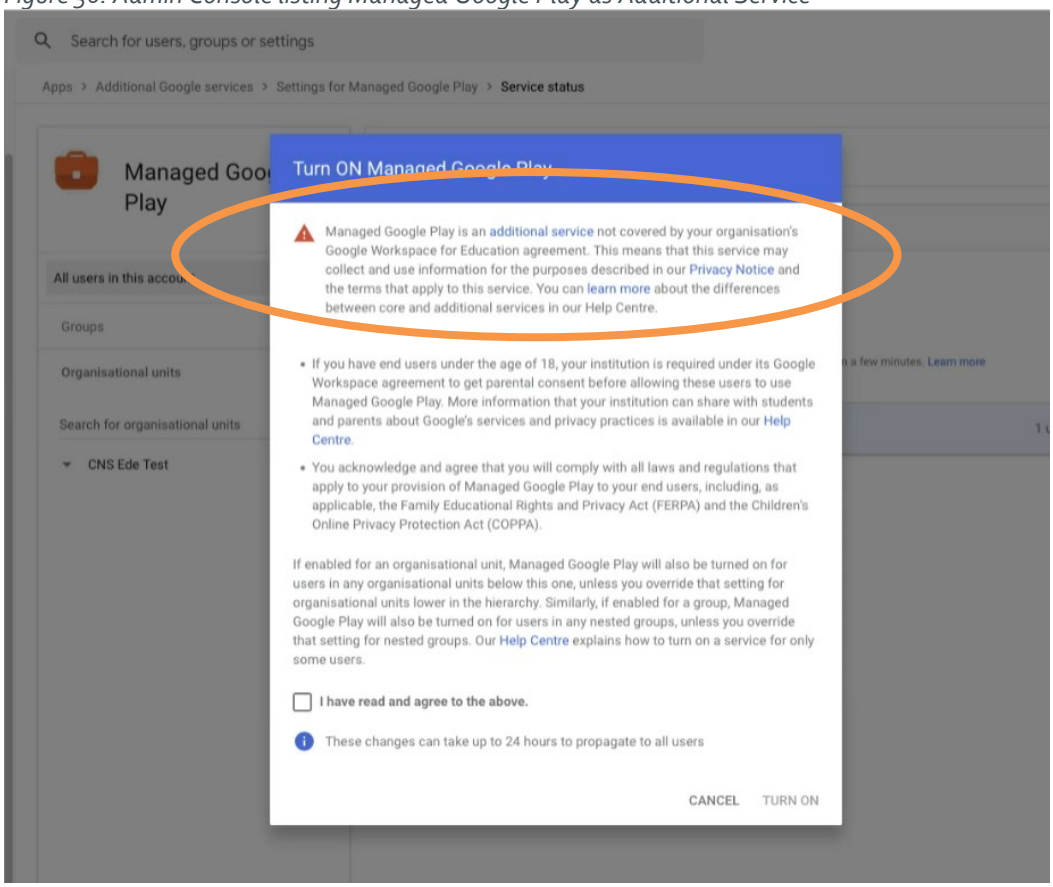
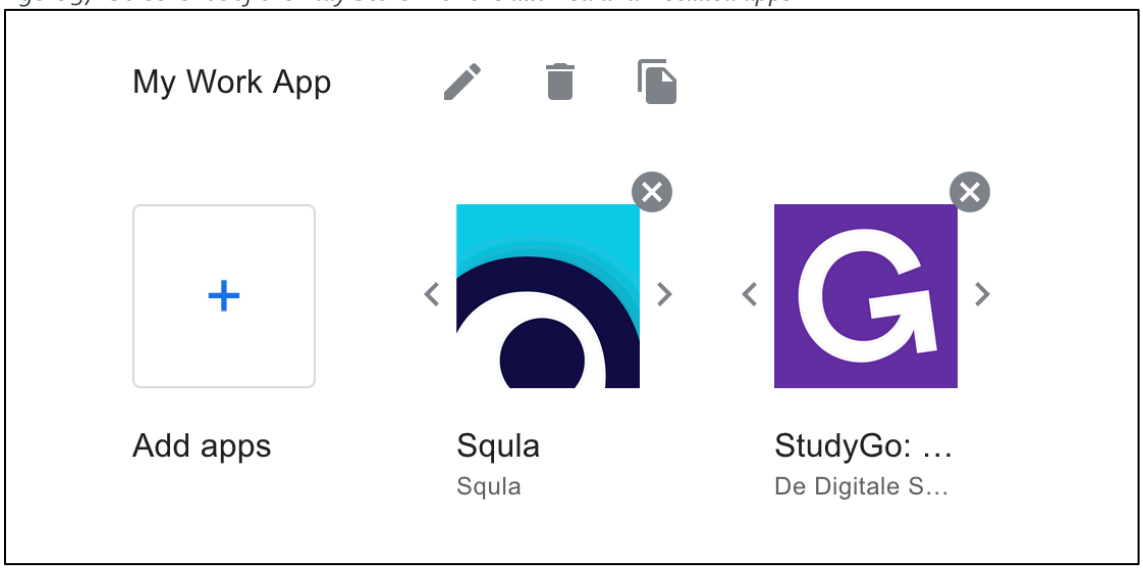


Figure 37: Screenshot of the Play Store with the allowed and installed apps[77]



[76] Screenshot made in the admin console of the school test account, 7 December 2023.
[77] Screenshot made 7 December 2023 in the test tenant.

However, none of the other options of the Play Store are available. End users cannot download other apps, or review apps.

6.2 Assessment

Google continues to act as an independent data controller for many relevant personal data in the *managed* Play Store, also if schools have signed the processing agreement for Chrome OS and the Chrome browser. It follows from Google's public documentation on the Managed Play Store, the Managed Play Agreement, that Google only wishes to process the Content Data as a processor, not other personal data Google processes about observed behaviour and the usage of the services.

Google does not provide any technical documentation about the Diagnostic Data in publicly available documentation, and permits itself as data controller to process the data about the use of apps for its own commercial purposes. The help articles about the ChromeOS data processor mode do not provide any information about this either, other than the general explanation that the processor agreement only covers the Essential Services.

The improved data processing agreement for Workspace with the Dutch schools and universities does not apply to the personal data collected by Google when an end user downloads an app from (managed) Google Play. Similarly, the new data processing agreement for managed ChromeOS and the managed Chrome browser does not apply to this data processing.

If schools wish to enable students to use selected allowed apps, they must distribute these apps via their own network. For browser extensions they can apply Force install, without users having to visit the Chrome webstore.

Appendix 1 – Essential Chrome Services[78]

Service name	Chrome browser	ChromeOS	Description
Accessibility—Image Annotation	✓	✓	Image Annotation allows visually-impaired users to read text in images.
Accessibility—Speech-to-Text	✓	✓	Speech-to-Text converts speech into text.
Accessibility—Text-to-Speech	✓	✓	Text-to-Speech converts text into natural-sounding speech.
Application Platform Metrics		✓	Application Platform Metrics measures ChromeOS app usage, and is tied to a pseudonymous identifier.
Autofill (excluding payment information)	✓		Autofill helps users fill out forms automatically with saved info, like your addresses. When you enter info in a new form online, Chrome might ask you if you'd like Chrome to save it.
Calculator		✓	The Calculator app provides users with simple calculation functions on ChromeOS devices.
Camera app		✓	A built-in camera app to provide high-quality camera experiences across the ChromeOS ecosystem.
Canvas app		✓	A built-in drawing app for Chromebooks that syncs drawings to a user's Google Account, so that they can be accessed from different devices.
Cast Moderator	✓	✓	Google cast moderator is a casting solution built specifically for Chrome users in the classroom. As an admin, you can set up a cast moderator for your school to allow teachers and students to share their screen wirelessly to a central display, using a secure access code.
Chrome Sync	✓		Chrome Sync saves a user's bookmarks, history, passwords and other settings to their Google Account, so that they can easily log in to other devices without needing to recalibrate the browser from scratch.

[78] Google Chrome Enterprise and Education Help, List of Essential (Chrome) Services, undated, page last visited 21 February 2024, URL: https://support.google.com/chrome/a/answer/13598068.

Chrome Update	✓		Update Service Chrome Update ensures that the latest version of Chrome is distributed, with the latest security updates and protections.
Chrome Variations	✓		Update Service Chrome Variations is the framework used to roll out or roll back individual Chrome features, and to ensure they're working as intended.
Chromebook Recovery Utility		✓	Chromebook Recovery Utility is a Chrome extension that lets users burn a recovery image onto a recovery device (e.g. USB drive, SD card) with which they can recover a ChromeOS device in recovery mode.
Crash Reports	✓	✓	Crash Reports are used by Google to identify and prioritize fixes for Chrome.
Cursive app		✓	A built-in notebook app for Chromebooks that syncs notes to a user's Google Account, so that they can be accessed from different devices.
Enrollment/Device Verification		✓	Enterprise Enrollment is a process that marks a device as belonging to a particular organization, thereby enabling the setting of device policies by IT admins in the Google Admin console.
Files app		✓	A built-in file app for Chromebooks to provide an entry point for other apps, such as gallery, audio player, and the video players.
Google Drive Syncing		✓	Google Drive Syncing is the process of downloading files from the cloud and uploading files to the cloud from a device's hard drive. After syncing, the files on a device match those in the cloud, to allow easy and convenient storage, access, and editing.
Kiosk Mode		✓	Kiosk Mode is a session that runs a single Chrome/Android app, after IT admins enrol a ChromeOS device into an organization and turn on Kiosk Mode.
Location Services		✓	Location Services on Chromebook estimates a user's geolocation. This is then used for tasks such as setting timezones, providing websites in the correct language, and alerting users to possible unauthorized log-ins.

Managed Guest Sessions		✓	With managed guest sessions, multiple users can share the same ChromeOS devices without having to sign in to their Google Account. Instead, they can sign in using a managed guest session.
Password Manager	✓		Password Manager supports users by saving and updating credentials, filling credentials into forms, and generating random and unique credentials.
Permission Suggestions	✓		Chrome Permissions Suggestions Service (CPSS) is a Chrome browser service that simplifies safe decision making for permission requests.
Phone-as-a-Security-Key	✓		Phone-as-a-Security-Key (PaaSK) is a form of second factor for Corp Authentication. With PaaSK, Google can turn any compatible iOS and Android device into a Security Key, to help protect your account.
Policy Management		✓	Policy Management allows IT admins to set policies for their enrolled managed devices, or for their managed end user Google Accounts (Chrome profiles).
Quick Answers - Translation		✓	Quick Answers - Translation allows users to translate content into their selected language, without needing to navigate elsewhere.
Safe Browsing	✓		Safe Browsing helps protect against known phishing, social engineering, malware, unwanted software, malicious ads, intrusive ads, and abusive websites or extensions.
Safe Sites	✓		Safe Sites uses the Safe Search API to inspect URLs for explicit content and prevent access by unauthorized users.
Screencast		✓	Screencast allows users to create and view screencasts. They can then upload them to Google Drive.
Spell Check (Basic)		✓	Spell check helps users to review and correct spelling errors when they enter text into input fields on the web. Basic spellcheck uses a dictionary stored locally on the device, text is not sent to Google.
Spell Check (Enhanced)	✓	✓	Enhanced Spell Check is used in Google Search and sends the text users enter into text boxes on webpages in their browser,

			to Google, for improved spelling suggestions.
Time Services		✓	Time Services on Chromebook relies upon Location Services to estimate your timezone.
Translate	✓		Allows the translation of web pages from one language to another.
User Metrics	✓	✓	User Metrics sends usage statistics to Google, to ensure features and services are improved and working as intended.
User & Device Reporting		✓	User & Device Reporting allows IT admins to view insights about the ChromeOS devices in their organization, such as Chrome devices count by version and the Chrome release channel of their devices.