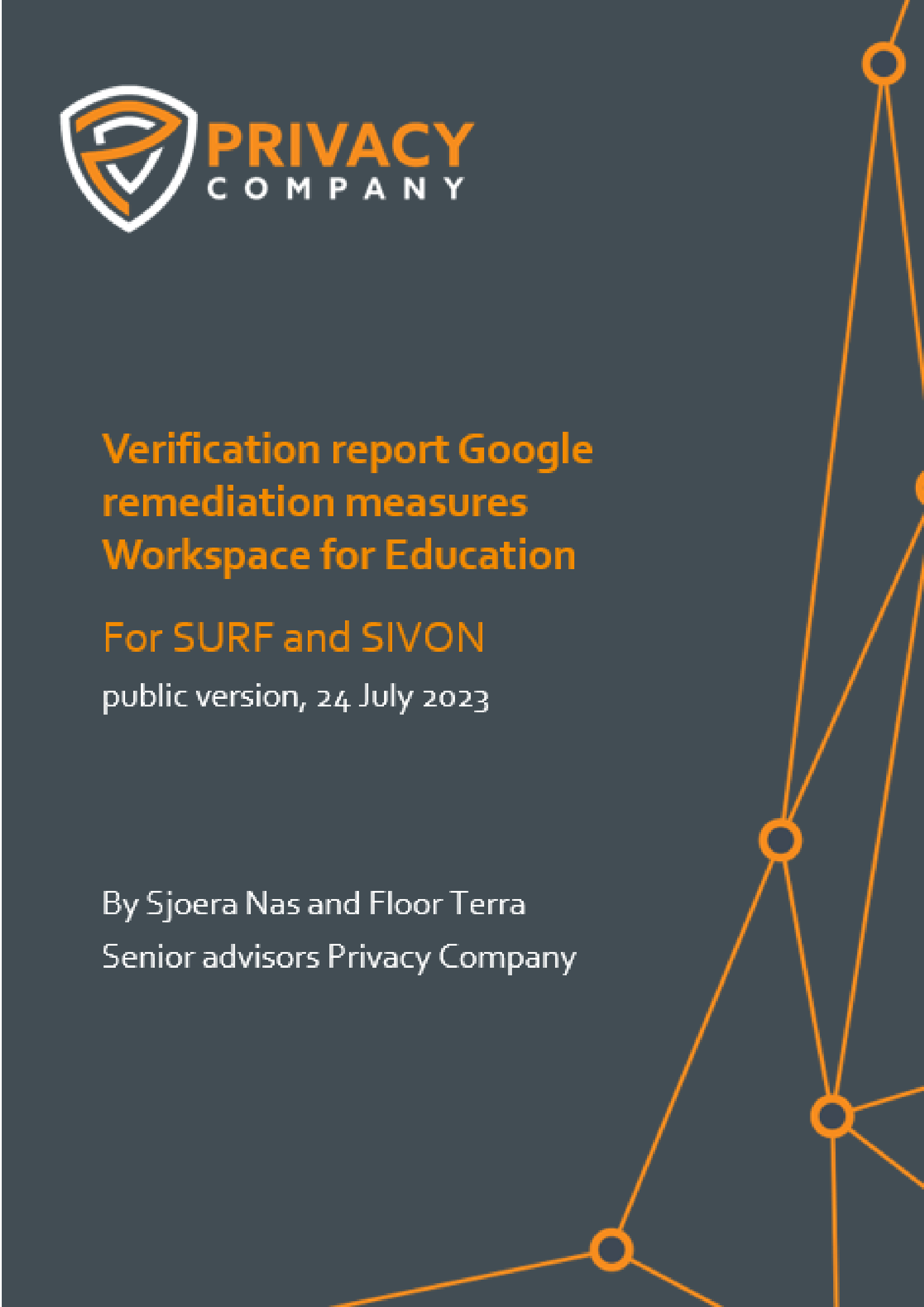
PRIVACY COMPANY

Verification report Google remediation measures Workspace for Education

For SURF and SIVON

public version, 24 July 2023

By Sjoera Nas and Floor Terra
Senior advisors Privacy Company



Summary

In August 2021 SURF and SIVON (the IT procurement organisations for schools and universities in the Netherlands) negotiated an improved agreement with Google for Workspace for Education, with an addendum on the Google Cloud Privacy Notice (the Privacy Amendment). In August 2021 they published an Update DPIA report with agreed remediation measures to mitigate the remaining high risks.

At the request of SURF and SIVON Privacy Company has verified if Google has taken the agreed remediation measures due by 9 June 2023.

During this verification, the researchers came across a number of potential new risks. SURF and SIVON are discussing these issues separately with Google in a structural dialogue about compliance.

Conclusion

The table below gives an assessment in colours. Most boxes are green. **This means Google has effectively mitigated the high risks on 9 June 2023,** or reduced them to a low risk. There are also two light blue coloured boxes with regard to transfers of personal data to third countries. SURF and SIVON are analysing those transfer risks in a separate project with Google, together with the procurement officers of the central Dutch government (*SLM Microsoft, Google and Amazon Web Services Rijk*[1]) in the context of a Data Transfer Impact Assessment (DTIA).

Table 1: 9 high risks identified in the Update DPIA, agreed measures Google, and verification results

No.	Risk	Agreed mitigating measure Google	Factual measure
1, 2	**Lack of purpose limitation Customer and Service Data**	Google will only process Customer Personal Data and Diagnostic Data (including Account Data) as data processor, for three purposes, when necessary: *1. to provide, maintain and improve the Services and Technical Support Services (TSS) subscribed to by Customer;* *2. to identify, address and fix security threats, risks, bugs and other anomalies* 3. *to develop, deliver and install updates to the Services subscribed to by Customer (including new functionality related to the Services subscribed to by Customer).*	Risk mitigated by contractual measures in Privacy Amendment.
		Google will not process Customer Personal Data and/or Service Data for advertising purposes or for profiling, data analytics and market research.	Risk mitigated by contractual measures in Privacy Amendment.
		7 purposes identified for which Google may further process Diagnostic Data as independent data controller. 1. billing and account management and customer relationship management and related correspondence with Customers and Customer Administrators; 2. improving and optimizing the performance and core functionality of accessibility, privacy, security and IT infrastructure efficiency of the Cloud Services and TSS; 3. internal reporting, financial reporting, revenue planning, capacity planning and forecast modelling (including product strategy); 4. abuse detection, prevention and protection (such as automatic scanning for matches with	* **Note**: wrong information Google in the proposed new GCPN addendum about agreed purposes. Low risk because the terms in the Privacy Amendment prevail over any information from Google.

[1] SLM Microsoft, Google Cloud en Amazon Web Services, URL: https://slmmicrosoftrijk.nl/.

		identifiers of CSAM, virus scanning and scanning to detect AUP violations); 5. processing of Personal Data in support tickets and support requests (including corresponding with Customers and Customer Administrators, and any attachments thereto) sent by Administrators to Google; 6. receiving and using Feedback; and 7. complying with legal obligations. For clarity, **the rendering of TSS is a processor activity**. Google will ensure that **other purposes in the Google Cloud Privacy Notice will not apply to the use of Workspace by Dutch schools and universities.** With regard to content scanning for Child Sexual Abuse Material (CSAM) and reporting 'hits' to NCMEC, Google will comply with applicable regulatory guidance from the EDPB.	
		Google assures that machine learning to improve the contents of data collected with the Spelling and Grammar check are limited to within the customer's own domain.	Google writes in its Workspace for Education Data Protection Implementation Guide: "*It is important to highlight that your Customer Data is not used to improve Spelling & grammar services for other customers' accounts.*"
		Definition of anonymisation included in the Privacy Amendment, in accordance with WP29 guidance on anonymisation techniques.	Risk mitigated by contractual measures in Privacy Amendment.
		The framework contract specifies how Google deals with *gagging orders* when ordered to disclose Content and Diagnostic Data to law enforcement authorities.	In Privacy Amendment and information in public whitepaper.
		Google will switch the default setting for Ads Personalization to Off for new end users (relevant for the use of *Additional Services*).	Correct default setting in Workspace for Education for new users.
3, 4, 7[2]	**Lack of transpa-rency Customer and Service Data**	Google will develop an inspection tool to provide access for admins to the Telemetry Data, including use of Features	Google has developed a Diagnostic Information Tool (DIT) that shows telemetry events (which may include Content Data). The time period of access only covers the last 24 hours, due to long recovery time.
		Google will publish a Help Center article detailing categories and purposes of the processing of diagnostic data (including data collected from cloud servers and telemetry events (atoms) from Android	Google has published a new explanation page about the DIT and the contents of the Telemetry Data. This page includes a general description of the retention periods. "*We retain most types of Service Data for a set period of up to 180 days.* (…) *In practice, diagnostic information is retained for shorter periods of between 30 to 63 days.* Google also refers to its Google Cloud Privacy Notice. This describes the 3 criteria Google applies to

[2] The risks were: Lack of Transparency Customer Data, Lack of Transparency Diagnostic Data, Lack of control third parties / processors.

			retain Service Data for longer periods. These are: 1. *Security, fraud and abuse prevention,* 2. *Complying with legal or regulatory requirements and* 3. *Complying with tax, accounting or financial requirements*
		Google confirmed that all subprocessors that process Diagnostic Data also process Customer Data and are therefore already included in the list of subprocessors for Customer Data. Google will provide details about its subprocessors, in particular for the Diagnostic Data. Google will specify ○ full entity name, ○ relevant Service(s), ○ location(s) where the data are processed, ○ activity (i.e., what does the subprocessor do, ○ whether the subprocessor processes Service Data in temporary, personal and/or archive logs.	Google has expanded the information about its subprocessors and affiliates, what personal data they can access for what purposes. **OUT OF SCOPE** The list of subprocessors includes companies and affiliates in third countries. Google is cooperating with the ongoing DTIA to assess the risks of transfer to third countries.
		Google will show an end user profile picture on the landing page for all Workspace Core Services (both web and mobile). This picture will disappear when the end user leaves the privacy protected Workspace services. Google commits to automatically log out regular Workspace-accounts when they visit disabled *Additional Services* and show a warning to K-12 users.	Google has applied the agreed measures. When *Additional Services* are disabled in a K-12 environment, Google shows a warning sign to end users when they wish to access these disabled services.
		Google will make all relevant legal information about the Google Workspace-account permanently available in an end user notice.	The pop-up is improved and personalised. While the relevant legal information is not permanently available through log-in or Google Account menu. Google has committed to make certain UI changes by [**date confidential**]
		Google will develop a Domain Wide Takeout capability to individual user level/org unit level.	Google has published information about the organisational Data Export at https://support.google.com/a/answer/12940323 and https://support.google.com/a/answer/100458 Data must be exported to the Google Cloud Platform. Google has ensured that the admin must accept the (processor) conditions from the Cloud Data Processing Addendum. For this use case GCP is not a Workspace *Additional Service*.
		Google provides a new warning to end users in the Feedback form not to share sensitive data with Google	Google shows a pop-up with a warning.
		Google will improve its explanation to admins in the Data Protection Implementation Guide that Google processes Account Data as a processor when the Google Account is used in the Core Services.	Google offers an explanation.

		Google will expand the availability of admin audit logs to cover all Core Services.	Google provides many more audit logs, in conformity with remediation plan - to the extent tested.
5, 6	**No legal ground for Google and schools/universities + Missing privacy controls**	With regard to the (separate) legal ground for the reading of cookie and telemetry data from end-user devices, as defined in the ePrivacy Directive, Google will follow regulatory guidance.	Google explains the necessity of the inclusion of Content Data in telemetry events about Spelling and grammar telemetry events in a separate topic on the new DIT information page, under *Spelling and grammar suggestions*. It is plausible that this data collection is exempted from consent under the Dutch analytical consent-exception.
		Google agrees contractually that end user consent is not applicable as ground for sharing Service Data with third parties when those parties' services are disabled by Customer (including Google as 3d party for *Additional Services*).	Included in the Privacy Amendment.
		Google will automatically log-out Workspace end users when they access (**enabled**) *Additional Services*.	Admins can disable access to all *Additional Services*.
		Google becomes a data processor for the Diagnostic Data, and for providing support, but not for the Feedback Data, and not for the data in Support tickets. Schools are advised to warn their employees not to use Feedback, and not to upload personal data in Support tickets, to prevent becoming joint controllers.	Google is data processor for the provision of TSS according to Privacy Amendment, but may also further process data in support tickets as data controller. Both the processing of Feedback Data and Support Data are agreed legitimate business purposes.
		Admins can prohibit the use of *Additional Services* when logged in with a Workspace Enterprise account.	Admins can disable access to all *Additional Services*.
8	**No access for data subjects**	Google to develop individual TakeOut tool	Google offers 3 different tools for admins and end users to export personal data (Data Export, Google Vault and Google Takeout). These tools are focussed on Content Data, with some activity logs (*Data owned by users*). These self-service tools do not provide access to all Service Data, but admins can export Diagnostic and Telemetry Data, and end users can use Google's DSAR form to request access to personal data Google processes as data controller (see 2 rows below).
		Google does not provide individualised access to Diagnostic Data, Telemetry Data and webserver access logs/cookie data (Google calls these data Service Data). Admins can collect some Diagnostic Data by exporting the expanded audit logs, and query for individual user data. The DIT only provides access to the last 24 hours.	Admins need to use BigQuery to export audit logs. Google has ensured that the admin must accept the (processor) conditions of the Cloud Data Processing Addendum. For this use case GCP is not a Workspace *Additional Service.* Google also enables super admins to request access to historical Telemetry Data.

		Google will publish details why it generally cannot provide access to Telemetry Data, Website Data and personal data from Google's SIEM security logs. Google has confirmed it will consider each request under Article 15 GDPR (i.e. no rejection by default).	New explanation published under *Information not provided in response to an access request*.
		The design of Google's DSAR form is not user friendly: users do not know what categories of data Google processes	Schools and universities can use the explanations in this report to help employees and students request access to all of their personal data, through self-service tools, through their admin, and through Google's DSAR form.
9	**Transfer of personal data to the USA + lack of control over sub-processors**		**OUT OF SCOPE**: The potential risks of transfer are assessed separately in the ongoing DTIA.

Contents

Introduction

At the request of SURF and SIVON (the IT procurement organisations for schools and universities in the Netherlands)[3], Privacy Company has verified that Google has taken the agreed remediation measures due on 9 June 2023 relating to Google Workspace for Education, in response to the risks described in the June 2021 update DPIA.[4]

During this verification, the researchers came across a number of potential new risks. SURF and SIVON are discussing these issues separately with Google in a structural dialogue about compliance.

Structure of this report

The table below first repeats the risks identified in June 2021 and the proposed mitigating measures. Not all proposed measures were necessary. Those measures are not repeated in the table below.

Nine separate sections below assess for each risk (by type of personal data) what measures Google has actually taken, and whether those measures are effective.

Terminology

In August 2021 SURF and SIVON negotiated an improved agreement with Google. The Privacy Amendment identifies two types of personal data: *Customer Data* and *Service Data*. Customer Data are the personal data that customers actively enter, receive and create themselves, such as file and email content. In the DPIA these data are called 'Content Data'. Service Data are any other personal data that are generated when using Google Workspace for Education. The update DPIA describes four types of Service Data:

1. Account Data
2. Support Data
3. Diagnostic Data / log files created on Google's servers containing data on individual use of the services (*service generated server logs*). Google calls these data *Service Data*.
4. Telemetry Data / subset of Diagnostic Data, messages containing data about user actions that are regularly sent from the user's devices including their browsers to Google via the Internet. Google refers to these data as *Diagnostic Data*.[5]

Google offers two types of services: *Core Services*, which are part of the Workspace for Education package, such as Docs, Sheets, Slides, Sync and Classroom, and *Additional Services*, which are outside of the agreement, such as YouTube and Search.[6] Based on the negotiated Privacy Amendment, Google processes all personal data from the Core Services as data processor. However, Google remains a data controller for the *Additional Services*.

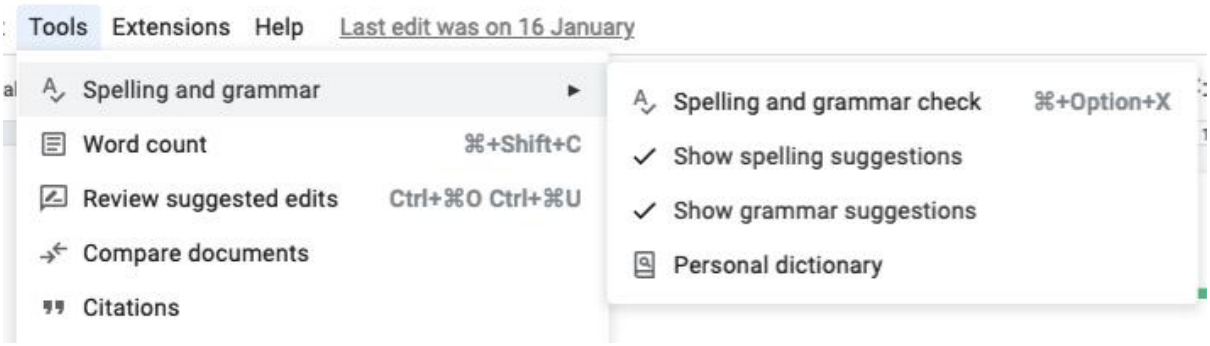
This report uses the term '*Spelling and grammar check*'. This is a built-in Feature in Google Workspace that processes Customer Data (Content Data) on Google's cloud servers. Google acts as a data processor for Features in Workspace. End users can choose not to have *Spelling and grammar check* suggestions displayed by Google, but system administrators cannot centrally disable the use of Workspace *Spelling and grammar check*.

---

[3] See for more information SURF, URL: https://www.surf.nl/en and SIVON, URL: https://sivon.nl/.
[4] Both the update report and the original DPIA are published by SURF at URL: https://www.surf.nl/files/2021-08/update-dpia-report-2-august-2021.pdf and URL: https://www.surf.nl/files/2021-06/updated-g-suite-for-education-dpia-12-march-2021.pdf respectively.
[5] Google does not classify these four types of Service Data as separate data categories.
[6] Google Workspace Services Summary, URL: https://workspace.google.com/intl/en/terms/user_features.html (undated, last accessed 13 June 2023).

The DPIA Update explained that Google offers a total of three different spell checkers, also two different ones in the Chrome browser, a local and a cloud service. Those two types of spell checker in the Chrome browser are outside the scope of this verification report.

Figure 1: Screenshot of Workspace Spelling and grammar check in Google Docs



Scope of this verification report

This verification report covers both the free (Fundamental) and the paid (Standard and Plus) versions of Google Workspace for Education. The only two privacy relevant differences between the free and paid version are that paying customers can choose to store content data for certain Core Services in data centres in the EU, and have access to more security features, such as device management. For device management schools can also choose to procure the Education Upgrade License for Chromebooks. This will be addressed in the separate report on the Chrome OS and Chrome browser.

The Update DPIA report includes an appendix explaining the specific risks for minor users of Google Workspace for Education services. Minors at school (in the Netherlands under 16 years) are an especially vulnerable target group. They cannot be expected to implement privacy measures independently, nor do they have the ability to consent to, or refuse use of school facilities. Google has developed a special K-12 setting in Google Workspace for Education, intended for students up to 18 years old. By designating themselves as K-12, schools and universities benefit from the most privacy-friendly settings in Google Workspace for Education. Google has confirmed that it does not apply age verification: universities and vocational education institutions can, and are recommended to, also choose the K-12 settings to benefit from these privacy friendly settings. But choosing K-12 is not enough: only the paid Workspace for Education versions offer the necessary centrally enforceable privacy protections.

Out of scope

This verification report does not include a new legal assessment of the amended agreement that Google reached with universities and schools for Google Workspace for Education.

This verification report equally does not repeat the measures that schools and universities should take themselves to mitigate the high risks, such as turning off access to the so-called *Additional Services*. These are services that Google offers in a role as data controller. There are more than 50 of these services. Examples are YouTube, the Google search engines (Google Search and Google Scholar) and Google Maps.[7] In the K-12 environment, *Additional Services* are off by default: in regular paid Workspace for Education environments, access is on by default, but administrators can centrally disable access.

[7] Google, Turn on or off additional Google Services, URL: https://support.google.com/a/answer/181865.

Meanwhile, Google offers one new public processor agreement for both Workspace services and the Google Cloud Platform, the Cloud Data Processing Addendum.[8] The contractual arrangements between Google and educational institutions on Workspace for Education explicitly prevail over this new processor agreement.

Based on the Privacy Amendment, Google's Standard Contractual Clauses apply to the transfer of data to Google and its (sub) processors in third countries both to Content Data and to Diagnostic Data.[9] The new SCC and the new 10 July 2023 EU adequacy decision for the USA are out of scope, because the transfer risks are analysed in the separate ongoing DTIA project.

Finally, this report does not address the use of Chromebooks and the Chrome browser. At the request of SIVON, Privacy Company has performed a separate verification analysis.

Workspace for Education test environments

To check Google's remediation measures, Privacy Company used a test environment with Google Workspace for Education Plus. The license was in the name of primary school CNS-ede and was set to K-12, i.e., Google's most privacy-protective setting for children under 18. Privacy Company tested on 23 and 26 January 2023.

Privacy Company requested and received additional information and screenshots on 27 January 2023 from the University of Groningen about the default settings and capabilities for admins to export personal data in the regular Google Workspace for Education Plus (which was not set to K-12).

[8] Google Cloud Data Processing Addendum, last modified 20 September 2022, URL: https://console.cloud.google.com/tos?id=dpast#dpst_customers.

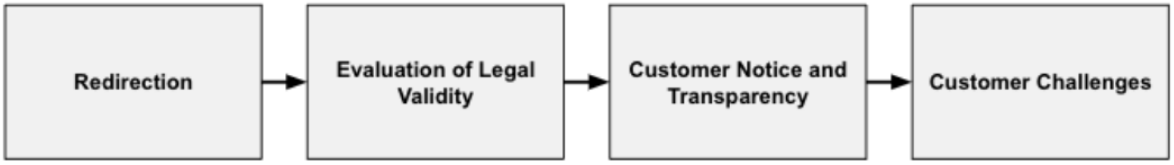
[9] Google sent an email in December 2022 to all school administrators in the Netherlands covered by the enhanced agreements with a supplement to the agreement, with a link to the Addendum on the Google Cloud Privacy Notice that includes the new SCC. [**URL confidential**]. As mentioned below, this text contains factual inaccuracies with regard to the agreed purposes of the data processing.

High risk 1: Lack of purpose limitation Customer Data

Google has agreed to contractual guarantees to mitigate the data protection risks resulting from the lack of purpose limitation for the processing of the Customer Data mentioned in Table 1 above. The agreed list of purposes is included in the Privacy Amendment with SURF and SIVON, in sections 6.1 and 6.2 of the Workspace for Education online Agreement.

When it comes to Google's handling of government orders for compelled disclosure, Google published a whitepaper explaining the steps it takes when it receives an order.[10] This whitepaper is limited to 'Customer Data', but under the Privacy Amendment, these safeguards also apply to claims for other personal data, such as Telemetry Data and Diagnostic Data from service-generated cloud server logs.

Figure 2: Diagram Google handling government requests for customer information



Conclusion: first high risk mitigated

Google has mitigated the first high risk through contractual measures.

High risk 2: Lack of purpose limitation Diagnostic Data

Similar to the measures to impose purpose limitation for Customer Data, Google has agreed to contractual measures to mitigate the data protection risks for Diagnostic Data. Google has agreed to become a data processor for the Diagnostic Data (service generated server logs and Telemetry data), the Support Data and the Account Data. The Privacy Amendment with SURF and SIVON amends the Google Cloud Privacy Notice in which Google lists different processing purposes for the Service Data.[11] The Privacy Amendment states that Google may process the (broadly defined) Service Data as a processor for the agreed three processor purposes. The Privacy Amendment also includes an exhaustive list of 7 agreed further processing purposes, when Google is permitted to process some Diagnostic Data as a controller for its own legitimate business purposes, when necessary.

The list was published in the public Update DPIA report of 2 August 2021.[12] In a separate mailing to school administrators in the Netherlands about the agreed purposes, Google has included a commercial purpose not permitted in the Privacy Amendment.[13] This added purpose is to send recommendations to optimise the use of Cloud Services, and to evaluate customer responses to such recommendations. In Dutch the explanation says:

> "*Om aanbevelingen te doen om het gebruik van Cloud Services te optimaliseren. Wij gebruiken Servicegegevens om u en onze klanten aanbevelingen te doen (bijvoorbeeld suggesties om uw account of gegevens beter te beveiligen, servicekosten te verlagen of prestaties te verbeteren, of uw configuraties te optimaliseren) en informatie te verstrekken over nieuwe of gerelateerde producten en functies met*

[10] Google whitepaper, February 2022, Government Requests for Cloud Customer Data, URL: https://services.google.com/fh/files/blogs/government_access_technical_whitepaper.pdf.
[11] Google Cloud Privacy Notice, version 25 January 2023, URL: https://cloud.google.com/terms/cloud-privacy-notice.
[12] Privacy Company for SURF, Update DPIA report Google Workspace for Education, 2 August 2021, URL: https://www.surf.nl/files/2021-08/update-dpia-report-2-august-2021.pdf.
[13] Google for Education, **confidential** addendum on the Google Cloud Privacy Notice, as negotiated by SURF and SIVON.

betrekking tot Cloudservices waarop onze klanten zich abonneren. We evalueren ook uw reacties op onze aanbevelingen (...)."[14]

Based on the Privacy Amendment Google is not allowed to process the Workspace for Education Service Data from Dutch customers in the education sector for this purpose. The Privacy Amendment does allow Google to send notifications to users about updates of the subscribed cloud services, and other notifications with regard to the subscribed cloud services, but this exception does not allow for the use of individual or tenant-level Service Data to send or evaluate responses to personalised recommendations, or use these personal data for the broad purpose of 'optimising the use of the services'. Google mentions three examples of optimisation, but these are not limitative, as the sentence starts with the term 'for example'. The term 'optimisation' may both refer to economical optimisation from the perspective of Google, as to improved usability from the perspective of end-users.

*Table 2: [**Confidential** - comparison]*

The differences in the information provided by Google are qualified as a low risk because the terms of the Privacy Amendment prevail over any information Google publishes or otherwise provides to schools and universities in the Netherlands.

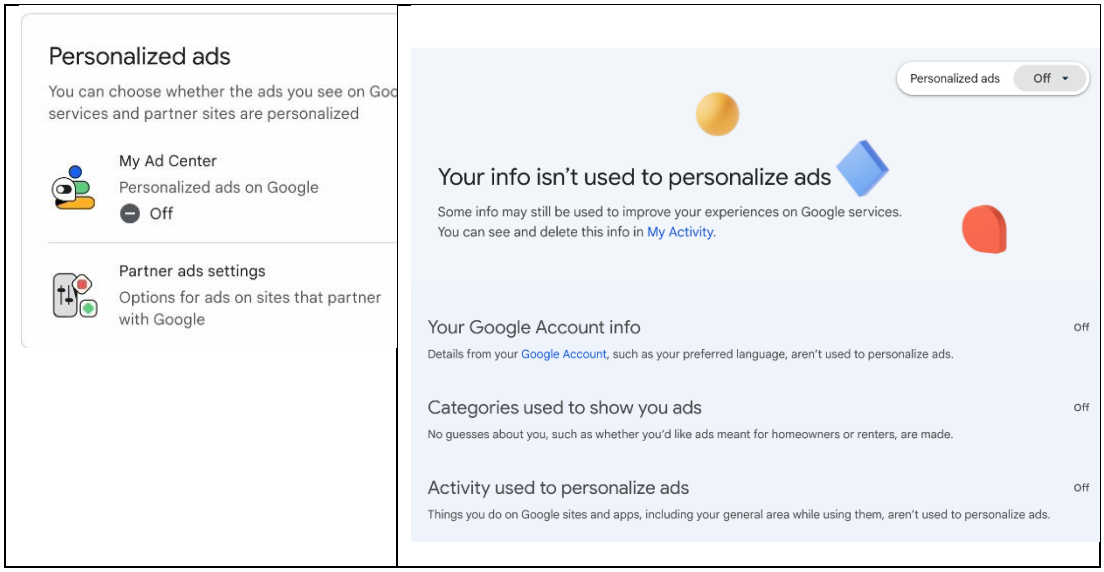
The agreement explicitly states that Google may not seek consent from end users to share Service Data with third parties if those services are disabled by school and university administrators. This includes Google as a third party controller for the *Additional Services*.

In the K-12 test environment, the default setting for ads personalisation is off, i.e. in accordance with Google's public commitments. In addition, Privacy Company checked the default settings in a new Google Workspace account in the University of Groningen's Workspace for Education Plus license. There too, ads personalisation is off by default, in accordance with the agreed remediation measure.

Figure 3: Screenshot of new user settings in Workspace for Education Plus K-12 environment

[14] Idem.

Figure 4: Screenshot default setting ads personalisation in university Workspace for Education Plus account



Conclusion: second high risk mitigated

Google has mitigated the second high risk through a combination of contractual and technical measures.

High risk 3: Lack of transparency Customer (Content) Data

Google had agreed to five technical measures to mitigate the risk of loss of control through a lack of transparency about the Customer (Content) Data.

1. Development of a tool to view Telemetry Data.
2. New warning in the Feedback form not to share sensitive data.
3. A visual reminder to end users using a profile icon whether they are working in the protected Workspace for Education environment, or outside it.
4. Make all relevant legal information about the managed Google Workspace account permanently accessible.
5. Explain in the Workspace for Education Data Protection Implementation Guide that Google processes the Account Data as a processor.

1. Development of a tool to view Telemetry Data.

The first measure was the development of a tool to view the contents of the Telemetry Data. Google has developed a tool for system administrators called the Diagnostic information tool (DIT).[15] [**Confidential**] See Figure 5 below.

*Figure 5: [**Confidential** - screenshot of DIT]*

Privacy Company tested the tool and analysed the telemetry events. In some telemetry events, Customer (Content) Data were visible, from the Workspace Spelling and grammar check. See the

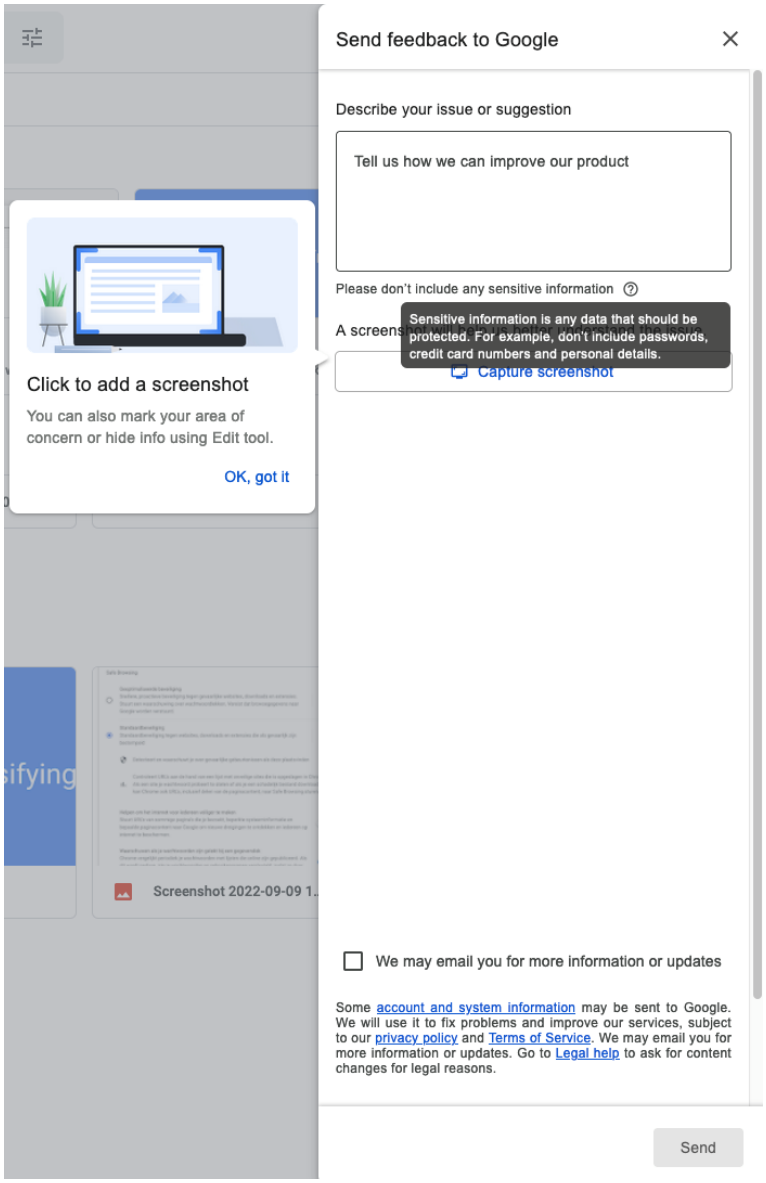
[15] Google, Diagnostic Information Tool, URL: https://support.google.com/a/answer/12830816

full content of such a message in the Annex with this report. The functioning of the DIT and its assessment are discussed in more detail under high risk No 4, below.

2. New warning in the Feedback form not to share sensitive data.

The second measure was a new warning in the Feedback tool to users not to share sensitive data with Google. The warning is necessary because the Privacy Amendment allows Google to further process the voluntary input in the Feedback form from end users for its own legitimate business purposes as controller. Google did include such a warning as shown in Figure 6 below.

Figure 6: New warning when filling in feedback form



3. Visual reminder to end users with the profile icon

The third technical measure was a visual reminder to end users with a profile icon whether they are working in the protected Workspace environment, or outside of it, in, for example, in a Google *Additional Service* such as YouTube or Search. As shown in Figure 8 below, Google does remove the icon when a user accesses an *Additional Service*. If access to these services is centrally disabled, students are automatically logged-out from their Workspace account, and the profile icon disappears.

Figure 7: Screenshot of profile icon in top bar browser when logged in using Kern Services

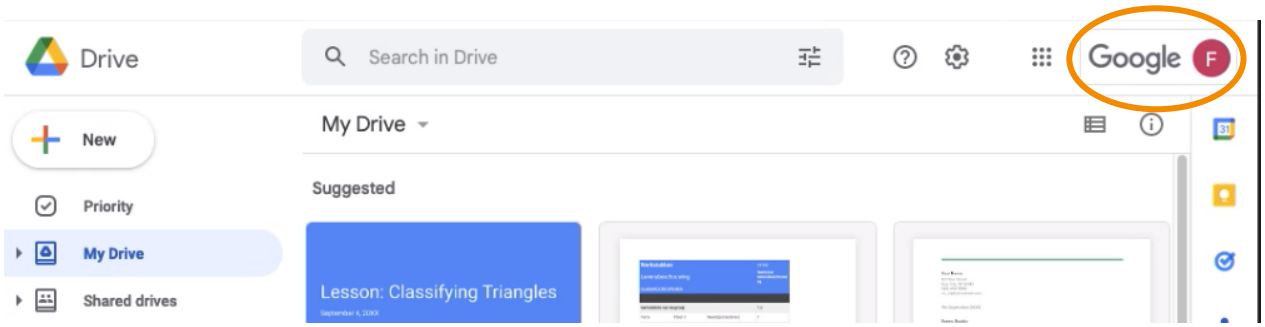


Figure 8: Screenshot of disappeared profile icon in top bar browser when using 'disabled' Additional Service Search

This practice is consistent with Google's public explanation on the use of *Additional Services*. Indeed, Google explains in its *Google Workspace for Education data protection implementation guide*[16] that users can still use some *Additional Services* such as YouTube if the administrator has centrally disabled access, but the user is then automatically logged out ("*use in a logged out state*").

Figure 9: Screenshot explaining Google about using Additional Services in Workspace for Education [17]

> **Note:** Even if a Google Workspace for Education admin has turned an Additional Service "Off", users may still access and use some Additional Services in an unauthenticated state or retain some limited functionality, for example, for purposes of accessing purchased content. For example, if the admin has disabled YouTube in the Admin console for the organization, a user can still visit YouTube and use the service in a logged out state, but login using their organization managed Google Account will fail. In this case, Google will not process data that can be linked to the user's organization managed Google Account.

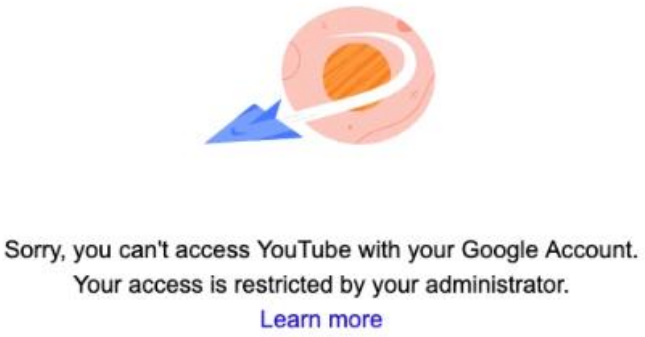
In the K-12 test environment, access to YouTube had been blocked. A user who wanted to access it anyway received a warning screen, as shown in Figure 10 below.

---

[16] Google Cloud Whitepaper, Google Workspace for Education data protection implementation guide, last updated February 2023, URL: https://services.google.com/fh/files/misc/google_workspace_edu_data_protection_implementation_guide.pdf .

[17] Idem, p. 11.

Figure 10: Warning screen that access to YouTube is disabled in the K-12 Workspace for Education environment



After the administrator of the K-12 test environment **turned on** YouTube access (which is off by default in the K-12 environment), users were able to use the service, and the profile icon disappeared, as agreed with Google.

Initially, Privacy Company did not succeed in disabling access in the K-12 test environment. This was due to the fact that there is a delay in the propagation of the settings. Google explains that it can take Google up to 24 hours to change the setting of an end user in the school environment.[18]

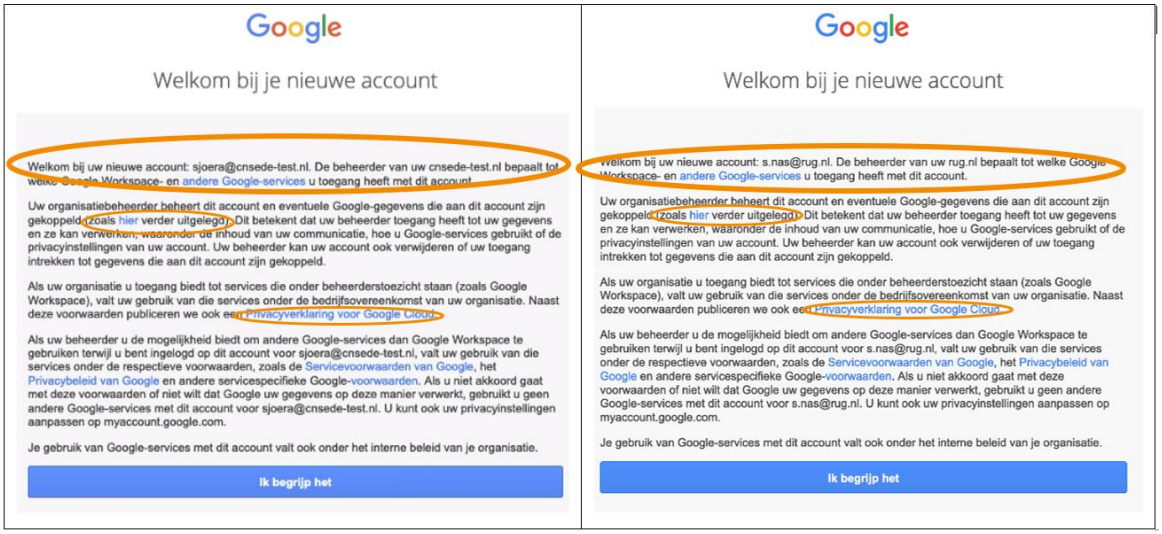
4. Relevant legal information permanently accessible

The fourth technical measure was the promise to make all relevant legal information about the Google Workspace account permanently accessible. End users can only read that information once, after the creation of a new account, in a pop-up screen with hyperlinks to a variety of legal documents. See Figure 11 below. The middle link, to the Google Cloud Privacy Notice, leads to a separate Google Cloud privacy statement. See

[18] Google, How changes propagate to Google services, URL: https://support.google.com/a/answer/7514107?hl=en .

Figure 12 below.

Figure 11: Welcome screens new user with reference to school and university role[19]

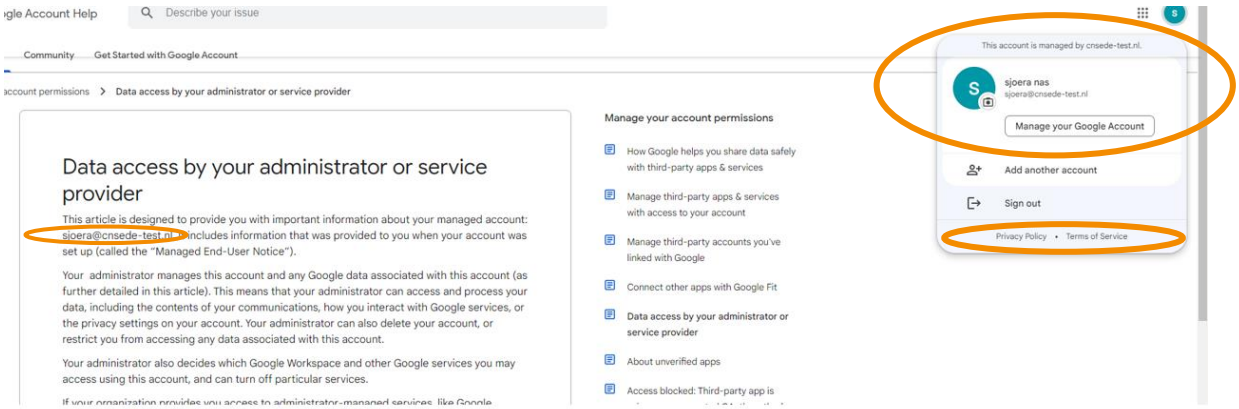


[19] The information shown to the new CNS-ede account was last checked on 12 June 2023. The information was unchanged.

Figure 12: Google Cloud Privacy Notice[20]

As a result of the negotiations with SURF and SIVON, Google has changed the information in the help center article that is referred to by the second hyperlink, *'zoals hier uitgelegd'*.[21] If a user is logged-in, the text in this article is now personalised and refers to the (1) Managed End User Notice, (2) Google Cloud Privacy Notice. See Figure 13 below.[22]

Figure 13: Screenshot of personalised help center article for logged-in K-12 user



Google did not (yet) make the information about the privacy rules for the managed accounts permanently accessible, or to remove the (incorrect) references to Google's (consumer) Privacy Policy and Terms of Service in the pop-up when a user clicks on the profile settings (see the right side of Figure 13 above). Google did add a new line on top of the screen

> *"This account is managed by [in this case:] cnsede-test.nl".*

[20] Google Cloud Privacy Statement, URL: https://cloud.google.com/terms/cloud-privacy-notice
[21] Google, Data access by your administrator or service provider, URL: https://support.google.com/accounts/answer/181692 .
[22] When Privacy Company tested the new information flow on 12 and 13 June 2023, the Dutch version of this text had not been updated, and was not yet personalised.

The pop-up continues to refer to two standard Google documents (i) Google's general privacy policy and (ii) Terms of Service, where Google acts as a data controller. In the university environment, Single Sign-on is used, and Google's legal information could not be found at all.

Figure 14: Login screen for new users in University Workspace environment

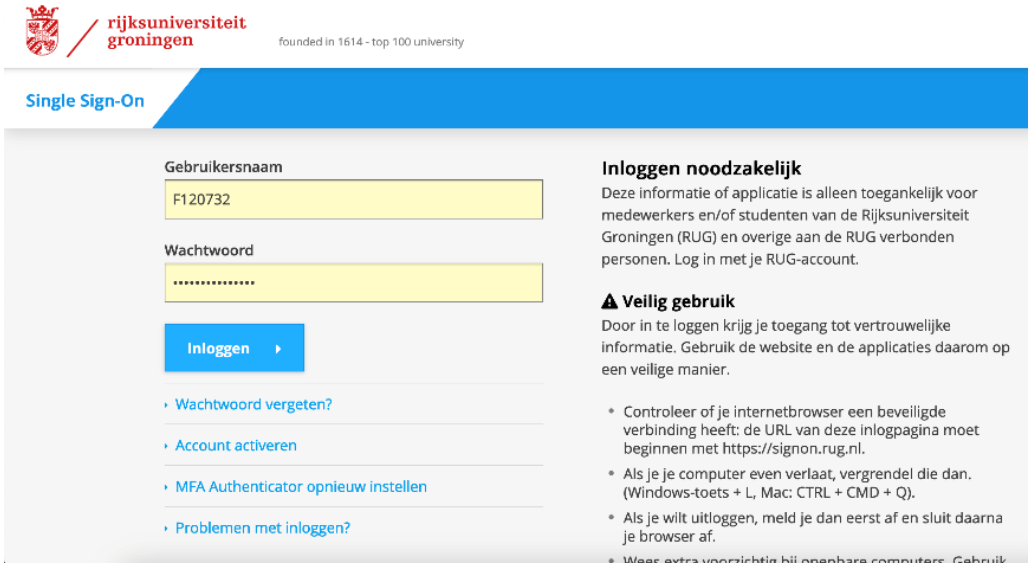


Figure 15: Screenshot Google Account menu for university Workspace account holders (top half)

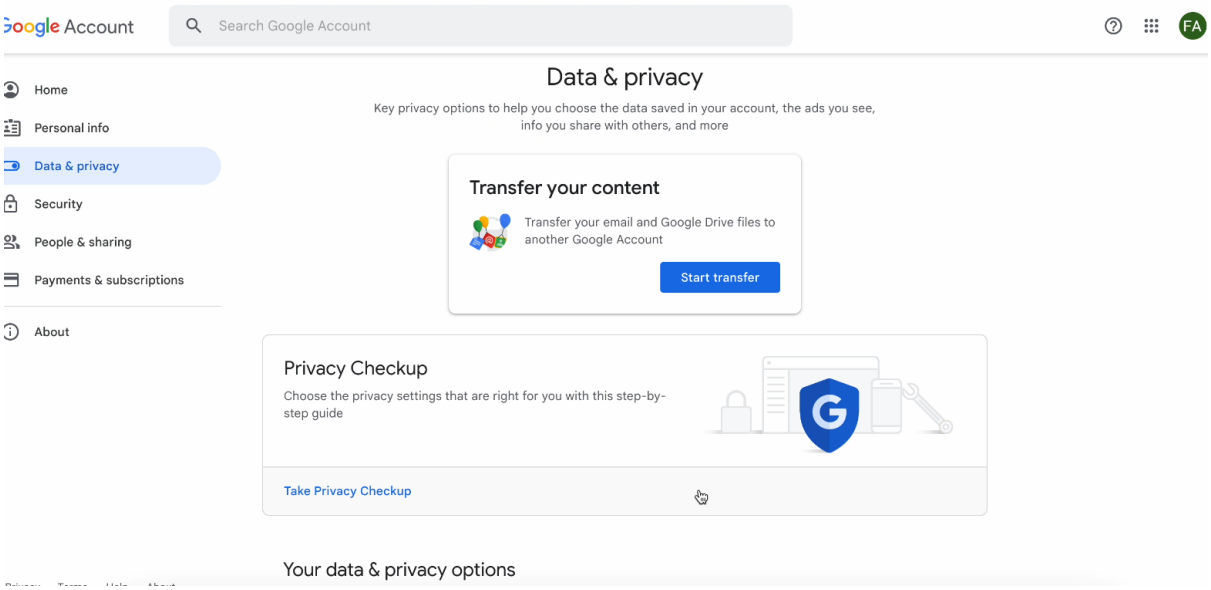
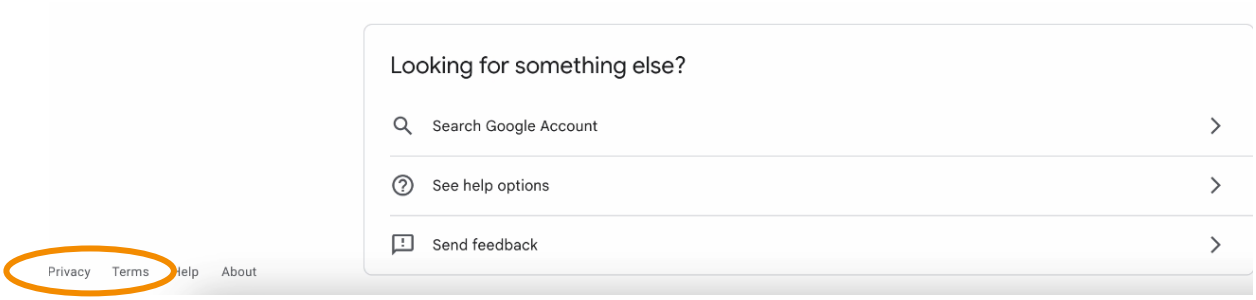


Figure 16: Screenshot of Google Account menu (bottom half)



Even in the Google Account menu, that contains all kinds of settings for the (managed Workspace for Education) Google account, there is no overview of the relevant legal sources. On the contrary, as depicted in Figure 16 above, Google shows links to its general privacy policy and terms and conditions at the bottom of this long page (thus acting as the data controller).

As a result of the negotiations with SURF and SIVON, Google has committed to make certain UI changes in the future, to ensure that managed account owners have permanent access to the correct legal information. This task will be completed by [**date confidential**]. [**Confidential**] In view of the interim solution to personalise the information about the access of the school admins, and Google's commitment to deploy a permanent solution [**confidential**] this element of this high risk is sufficiently mitigated.

5. Explain that Google processes the Account Data as a processor

The fifth measure was the promise to explain in the *Workspace for Education Data Protection Implementation Guide* that Google processes the Account Data as a processor when the Google Account is used in the Core Services. Google explains the Account Data in this guide, but you have to read between the lines to understand that Google can also process the Account Data as an independent controller for all the purposes in its general privacy statement when users log into the *Additional Services* with their school account.

Google writes:

> *"Users can provide information directly, when providing a name and profile picture, or indirectly, when Google collects information about when and for what purposes and in what context (app/web, platform and device) a user signs in. When a user signs in to their new organisation-managed Google Account you created, they receive a notice explaining how their data is collected and accessed by their admin, and how their use of Google Workspace for Education Core Services is governed by your organisation's Google Workspace for Education terms. The notice also explains that use of Additional Services when used with the organisation-managed Google Account are governed by Google Privacy Policy and Google Terms of Service, and applicable service-specific terms."*[23]

The term Account Data falls under Service Data and also includes device/browser data and unique identifiers, as well as, for example, log-in and log-out times or the times a user enters an incorrect password.

> *"[**Confidential**]"*[24]

Without a clear explanation from Google, users might also think that Account Data is part of Customer Data. This is the case with many paid services from other cloud providers. That explanation does appear in the Google Cloud Privacy Notice[25] , but it is not easy for end users to find, as the link to it appears only once in the pop-up screen after account creation.

Because the agreement with SURF and SIVON allows Google to further process the Service Data, which includes the Account Data, for 7 of its own purposes, it is important that Google clearly informs the organisations what it does with the names and e-mail addresses of end users. Based on the Privacy Amendment, Google may not use either Content or Service Data for profiling, for advertising, data analytics and market research.

To ensure students and employees are correctly informed about the scope and purposes of the processing by Google, schools and universities should explain to students and employees that Google is a processor for the Account Data. They can refer to the agreed processing purposes in the

---

[23] Google Workspace for Education data protection implementation guide, February 2023, p. 12.
[24] **Confidential** Google for Education Privacy Amendment for SURF and SIVON
[25] Google Cloud Privacy Notice, 25 January 2023, URL: https://cloud.google.com/terms/cloud-privacy-notice

confidential Table 2 above (different from Google's communication). Because schools and universities are the data controllers, they are in charge of the information obligations. As long as they use the correct information, the risk is sufficiently mitigated.

Conclusion: third high risk mitigated

Google has taken four successful measures to mitigate the third high risk, and has committed to take a fifth measure. The four successful measures are: the creation of the DIT tool, the warning in the Feedback tool, the visual reminder with the profile icon and the information about Google's role as processor for the Account Data. Schools and universities are responsible to inform their employees and students about the purposes for which Google may process the Account Data. With regard to the fifth measure, Google has committed to make the relevant legal information permanently accessible for end-users by [**date confidential**]. Until then, schools and universities can inform their employees and students with the information in the public DPIA and this verification report.

High risk 4: Lack of transparency Diagnostic Data

Google promised seven technical measures:

1. Public documentation of Telemetry Data;
2. Development of a tool to view Telemetry Data;
3. Expanded administrator access to Diagnostic Data via audit logs;
4. A Domain Wide Takeout tool that allows system administrators to easily answer a data subject's (pupil, student or employee) data subject access request;
5. List of sub-processors with their subsidiaries, and Google affiliates processing both Content and Diagnostic Data, with detailed information on the types of personal data they can process;
6. A visual reminder to end users using a profile icon whether they are working in the protected Workspace for Education environment, or outside it.
7. Make all relevant legal information about the managed Google Workspace account permanently accessible.

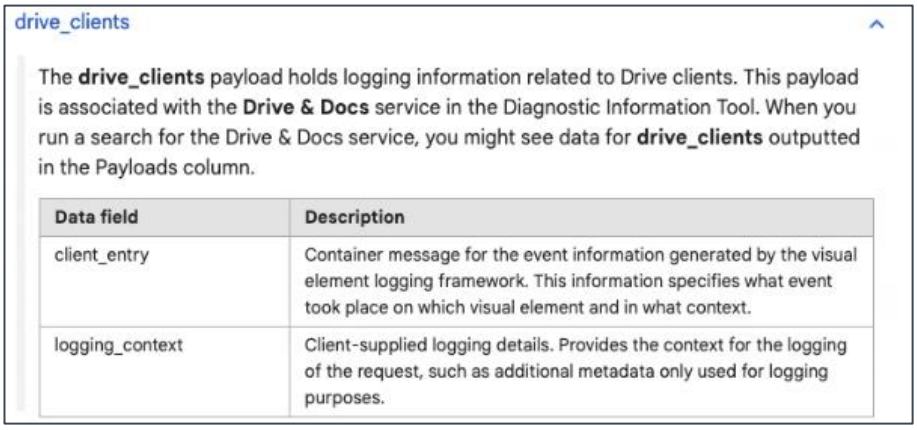
The last two measures have already been discussed above, and will not be repeated here.

1. Public documentation of Telemetry Data;

Google implemented the first measure to mitigate the fourth high risk in two phases. In December 2022, Google only published brief documentation with a description of some events. For example, Google's documentation on drive_clients only described only two fields. It was not transparent that the logging_context field could also contain Content Data. As shown in the Annex with this report, the telemetry event included a misspelled sentence, with the correct spelling.

> *"context: \""ididunt ut labore et dolore magna aliqua homework splelling"" suggestion: \"spelling".*

Figure 17: Google descriptive documentation of the telemetry event drive_clients



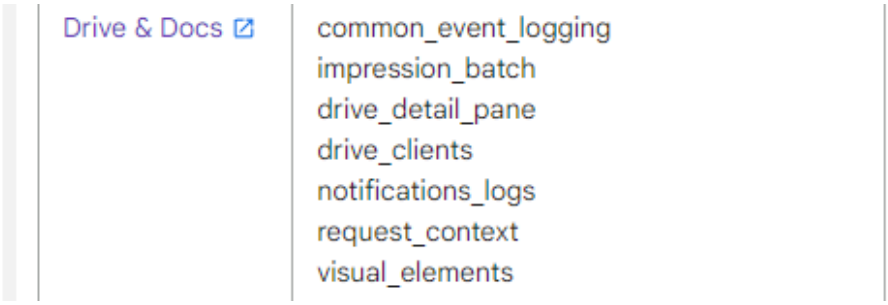
drive_clients

The **drive_clients** payload holds logging information related to Drive clients. This payload is associated with the **Drive & Docs** service in the Diagnostic Information Tool. When you run a search for the Drive & Docs service, you might see data for **drive_clients** outputted in the Payloads column.

Data field	Description
client_entry	Container message for the event information generated by the visual element logging framework. This information specifies what event took place on which visual element and in what context.
logging_context	Client-supplied logging details. Provides the context for the logging of the request, such as additional metadata only used for logging purposes.

On 9 June 2023, the second phase, Google has significantly expanded its documentation about Telemetry Data. The information page about the Diagnostic Information Tool[26] (DIT) contains two sources of information: a general description with non-exhaustive examples of telemetry events,[27] and detailed examples with the full payload of a representative browser telemetry event for each Workspace Core Service.[28] See Figure 18 and Figure 19 below.

Figure 18: New Google samples of representative events in Drive & Docs[29]



Drive & Docs

common_event_logging
impression_batch
drive_detail_pane
drive_clients
notifications_logs
request_context
visual_elements

[26] Google, Diagnostic Information Tool, URL: https://support.google.com/a/answer/12830816.
[27] Idem, 'Understand your search results'.
[28] Google, Payload examples for the Diagnostic Information Tool, URL: https://support.google.com/a/answer/13675570?sjid=5964413579470267587-EU
[29] Google, Diagnostic Information Tool, URL: https://support.google.com/a/answer/12830816

Figure 19: New Google example of the full contents of common_event_logging[30]


```
{"common_event_logging":"'{\"clientInfo\":{\"androidClientInfo\":
{\"applicationBuild\":\"2019999948\",\"board\":\"bluejay\",\"brand\":\"goog
le\",\"country\":\"US\",\"device\":\"bluejay\",\"deviceFingerprint\":\"goog
le/bluejay/bluejay:13/TP1A.XXXXX.004.A2/XXXXX:user/release-
keys\",\"extensionVersion\":[{\"extension\":33,\"version\":3},
{\"extension\":30,\"version\":3},
{\"extension\":31,\"version\":3}],\"gmscoreVersion\":223316044,\"hardware\"
:\"bluejay\",\"locale\":\"en\",\"manufacturer\":\"Google\",\"mccMnc\":\"404
49\",\"model\":\"Pixel6a\",\"osBuild\":\"TP1A.222093.004.A2\",\"product\":\
"bluejay\",\"radioVersion\":\"i12345-102852-220720-B-
321321321\",\"sdkVersion\":33},\"clientType\":\"ANDROID\"},\"clientTimestam
pMillis\":\"1664529600759\",\"deviceStatus\":
{\"isXXXXXDevice\":true},\"logSource\":\"CALENDAR_CLIENT\",\"timestampMilli
s\":\"1664529600760\",\"timezoneOffsetSeconds\":19800}'","calendar_client_e
vents": "'{\"visualElementEntry\":{\"ancestryVisualElement\":
{\"elementId\":92131},\"visualElementMetadata\":{\"clientMetadata\":
{\"channel\":\"PROD\",\"orientation\":\"PORTRAIT\",\"versionName\":\"2022.3
6.0-472143158-release\"},\"userMetadata\":
{\"userType\":\"EXTERNAL\"},\"userNotificationMetadata\":
{\"userNotificationContentState\":\"ORIGINAL\",\"userNotificationSource\":\
"EVENT\"}}}}'"}
```


In reply to the specific observations from December 2022, Google provided a paragraph with explanation why it is necessary for Google to collect Content Data in Telemetry Data about its Spelling and grammar check, and a complete sample of the payload of the common_event_logging event that accompanies each event as envelope.

Google explained that several processing operations take place both on the server-side and client-side to provide the Spelling & Grammar functionality to users. Google logs data for Spelling & Grammar on the user's client because users interact with the feature (e.g. user clicks accept/reject spelling or grammar suggestions) on the client side. As quoted in the Figure 20 below, Google has programmed the client (browser) to send the data to its own cloud servers to be able to verify that the feature is working properly.

Figure 20: Google new explanation about the Spelling and grammar check[31]

> Suggestions are presented to the user on their client device by underlining a word or phrase. When a user selects any of the spelling and grammar suggestions, the service presents them with one or more suggested edits and the option to ignore the suggestion. The service logs the user's selection on the client along with the relevant portion of the content used to make the suggestion. This logged data is sent to the server where it is then processed to ensure that this feature is working properly; logging which suggestions are accepted, rejected, or ignored is essential for the reliability, effectiveness. and functioning of this feature.

[30] Idem.

[31] Idem, https://support.google.com/a/answer/12830816#associations&zippy=%2Cwhich-google-workspace-services-are-included-in-the-diagnostic-information-tool%2Cwho-can-use-the-diagnostic-information-tool%2Cretention-of-diagnostic-information%2Cdata-aggregation-and-similar-measures%2Cexample-of-diagnostic-information-outputted-in-the-payloads-column%2Cspelling-and-grammar-suggestions.

Google publicly explains:

> *"Without this information, the spelling & grammar check feature would degrade over time and provide incorrect/sub-standard spelling & grammar suggestions which would adversely impact the reliability, effectiveness and functioning of this feature."*[32]

Google has also explained to SURF and SIVON that there are further scenarios such as when a user's client is in offline mode where the logging necessarily must happen on the client-side.

In the DIT documentation chapter about Content Data in Spelling and grammar check, Google includes a link to a blog about smart features in general.[33] Google confirmed that the chapter in the DIT documentation only relates to the feature Spelling and grammar check and not (also) to other features.

As additional mitigating measure Google explained that the maximum retention period of the Telemetry Data about the use of the Spelling and grammar check is 30 days.

As shown in the Annex, the event with the Spelling and grammar check contains a lot of so called 'experiment ID's'. It is not clear what these experiments are.

Google's documentation explains:

> *"experiment : Additional details about the experiments that are active, including the experiment IDs.*
>
> *Experiment_ID : This is the ID for the experiment."*

Under statutory law, Google is bound to comply with the ePrivacy rules. The Privacy Amendment contains specific arrangements in this respect.

Privacy Company also found other Content Data in two other telemetry events: (i) the email address of the researcher and (2) the name of the wireless earphones of the researcher.

The e-mail address is included in the entry "user_jid". Google documents this occurrence in the representative payload example about Meet as: redacted-email@redacted-domain.com and explains:

> *user_jid : The user JID of the participant. In this case, it is redacted-email@redacted-domain.com.*

Google does not document the occurrence of the collection of the name of the Bluetooth wireless earphones of the researcher. Since Google confirms in the DIT documentation that the information is a comprehensive view of the Telemetry Data collected by Google, and admins and end users can compare the data collection with the public documentation, Google apparently no longer collects this name. Privacy Company did not perform a retest of the Telemetry Data in the spring of 2023, and has not verified if Google has indeed stopped collecting the information about the earphones. Because of Google's confirmation that the documentation is comprehensive, this difference is not classified as a high risk.

Google has committed to provide sufficiently adequate documentation about the telemetry events to enable an auditor to compare the documentation with the collected data. With the expanded information, Google has successfully implemented the agreed measure and mitigated the high risk. The public documentation enables auditors to verify if the collection of Telemetry Data matches with

---

[32] Google explanation provided to SURF and SIVON.
[33] Google also referred to a blog from 2019 about the use of AI in the Spelling and grammar check, at URL: https://workspace.google.com/blog/productivity-collaboration/everyday-ai-beyond-spell-check-how-google-docs-is-smart-enough-to-correct-grammar

the documentation. The public documentation also allows admins and data subjects to compare the collected data with the public documentation. Admins can use the DIT tool to verify whether the Telemetry Data collected by Google correspond with the DIT documentation. Data subjects can verify this by submitting a Data Subject Access Request for Telemetry Data via their admin (through the DIT tool and additional form for (super)admins, see below). As a result, schools and universities can fulfil their GDPR transparency obligations as data controllers in relation to the Telemetry Data.

2. Development of a tool to view Telemetry Data;

The second agreed measure to mitigate the fourth high risk is the development of a tool to view Telemetry Data, the DIT. The DIT does indeed provide insight into telemetry data, for a list of Core Services, but only for up to the past 24 hours. Google explained it uses this short look-back period to be able to provide a reply within a relatively short time period. Admins can use the DIT every 24 hours if they want, to get a broader picture of Telemetry Data.

Google has explained that DIT shows telemetry from the following services, for both web, iOS and Android:

- Assignments (Google Workspace for Education only) (web only)
- Calendar
- Chat
- Classroom (Google Workspace for Education only)
- Cloud
- Search
- Contacts (web)
- Drive & Docs (Docs, Drive, Forms, Sheets, Slides)
- Gmail
- Groups (web only)
- Jamboard
- Keep
- Meet
- Sites (web only)
- Tasks
- Voice [out of scope DPIA]

*Figure 21: [**Confidential** - screenshot DIT]*

*Figure 22: [**Confidential** - screenshot DIT]*

Due to the short time frame for the DIT (maximum access only to the last 24 hours), the DIT cannot function as a data subject access request tool, as it does not provide full insights in all Telemetry Data Google processes. Most users do not use all Workspace services every day. The 24 hour period also does not provide insights in the factual data retention periods.

As a result of the dialogue with SURF and SIVON, Google developed two measures to mitigate this risk:

1. a more detailed description of retention periods (in addition to the retention information provided in the Google Cloud Privacy Notice),
2. a manual process for super admins to ask for access to older Telemetry Data in reply to a data subject access request.

New description of retention periods

The page about the Diagnostic Information Tool includes a description of the average retention periods of the Telemetry Data.

> *"We retain most types of Service Data for a set period of up to 180 days. (...) In practice, diagnostic information [Telemetry Data in this report] is retained for shorter periods of between 30 to 63 days.*[34]

With regard to the Content Data that may be part of some Telemetry events about the use of the Spelling and grammar check, Google applies the shortest retention period, of maximum 30 days.

Figure 23: Google explanation of retention period for Spelling and grammar telemetry events[35]

> These logs are temporary in nature, held for a maximum of **30 days**. They are collected, anonymised or pseudonymised, and aggregated to provide the information needed to operate the spell and grammar check tool. The document itself does not retain a record of spelling suggestions and interactions.

Google also refers to its Google Cloud Privacy Notice.[36] In this Cloud Privacy Notice Google writes:

> *"We retain Service Data for different periods of time, depending on the type of data, how we use it and how you configure your settings. When we no longer need Service Data, we delete or anonymise it. For each type of Service Data and processing operation, we set retention periods based on the purposes for which we process it, and ensure that Service Data is not kept longer than necessary.* ***We retain most types of Service Data for a specified period of up to 180 days (the exact number depends on the specific type of data).*** *However, some Service Data may be retained for longer periods if there is a business need to do so. We generally have longer retention periods (which may be more than one year) for Service Data retained for the following purposes: (...). "*

Google describes 3 criteria when Service Data are retained for longer periods. These are:

---

[34] Google, Diagnostic Information Tool, URL: https://support.google.com/a/answer/12830816.
[35] Idem, under 'Spelling and grammar suggestions'.
[36] Google Cloud Privacy Notice, 25 January 2023, URL: https://cloud.google.com/terms/cloud-privacy-notice

1. *Security, fraud and abuse prevention,*
2. *Complying with legal or regulatory requirements and*
3. *Complying with tax, accounting or financial requirements.*

By publishing the retention period of 180 days for Service Data, with a shorter retention period for telemetry events about the Spelling and grammar check of max 30 days, and a shorter period of up to 63 days for most Telemetry Data, Google has complied with the request to provide information about the retention periods.

Additionally, Google has provided the three criteria it applies to determine a longer retention period.

With this information about the retention periods and criteria, Google has mitigated this element of the risk of a lack of transparency of the Diagnostic Data. Google now enables the controllers (schools and universities) to comply with the (minimum) requirements of the transparency obligation about personal data indirectly collected from data subjects. Article 14(2) sub a of the GDPR specifies that controllers may suffice with explaining the criteria, if it not possible to provide the specific periods for which the data will be stored. It is plausible that retention for the purpose of security requires widely different retention periods, depending on the circumstances and nature of the security risk. With regard to the regular retention period for the Service Data, 6 months (180 days) is a relatively short period for Google to fulfil its obligations as processor, or to 'further' process these Diagnostic Data for the exhaustive list of agreed further processing purposes.

In all cases, Google has to comply with the agreed purpose limitations as processor, or as controller, when contractually permitted to process some personal data for its own legitimate business purposes, when proportionate.

New manual access to historical Telemetry Data

On [**date confidential**], Google enabled super admins from Dutch schools and universities to ask for available historical Telemetry Data. In the future all super admins will be able to make such requests via the Admin Console [**confidential**].

Google insists that admins must send Google a copy of the access request of their employee/student, to prove that they need access to the historical Telemetry Data.

Google explains:

> *"[**Confidential**]."*[37]

With the request to super admins to provide a copy of a Data Subject Access Request, Google wants to ensure that it provides the Telemetry Data in reply to a request of a verified data subject. Google is apparently concerned that an admin would randomly pick names of employees or students. This extra hurdle by itself does not lead to a (new) high risk, as long as the super admins carefully redact any non-necessary data from the Data Subject Access Request.

Google is finalizing the implementation of this new access procedure [**confidential**]. During this [**confidential**] period, [**confidential**]. The specific response time in each case will depend on the complexity of the request and the volume of diagnostic information to be produced.

*Figure 24: [**Confidential** - screenshot form]*

[37] [Confidential].

In sum, with the capability for super admins from Dutch schools and universities to ask for available historical Telemetry Data Google has mitigated this component of the high risk of lack of transparency about the Diagnostic Data.

3. Expanded administrator access to Diagnostic Data via audit logs;

The third agreed measure was expanding the availability of audit logs for system administrators. Google has implemented this measure, and makes 30 audit logs available (as tested on 23 January 2023). In the list below, the new logs are highlighted in green. Privacy Company did not test all Services for this verification report, which is why some logs were empty. For examples of logs with content, see the Annex.

Table 3: Overview of available audit logs

1. Access Transparency log events	2. Admin log events	3. Assignments log events
4. Calendar log events	5. Chat log events	6. Chrome log events
7. Chrome Sync log events	8. Classroom log events	9. Cloud Search log events
10. Contacts log events	11. Context-aware access log events	12. Currents log events
13. Device log events	14. Directory Sync log events	15. Drive log events
16. Google profiles log events	17. Graduation log events	18. Groups enterprise log events
19. Groups log events	20. Keep log events	21. LDAP log events
22. Looker Studio log events	23. Meet log events	24. Oauth log events
25. Password Vault log events	26. Rule log events	27. SAML log events
28. Takeout log events	29. Tasks log events	30. User log events

Google has terminated five audit logs: Login audit log, Token log, Hangout Chat log, Google+ log and Voice logs (Voice is out of scope of the DPIA).

The available audit logs contain all kinds of Content Data, such as file names and paths, or email subject lines, but that does not pose any additional data protection risks now that Google acts as a processor for these service-generated server logs.

As shown in Figure 25 below, Google publicly documents the retention periods for audit logs.[38] Google explains how long it can take for logs to become visible (between a few minutes and period of 1 to 3 days), and lists retention periods for all specific logs. In general, Google keeps audit logs for 180 days (six months). System administrators can extend that retention period by exporting them to their own storage space. If they use Google Cloud to store these exported data, for Google these data then become Content Data.

[38] Google, Data retention and lag times, URL: https://support.google.com/a/answer/7061566?hl=en.

Figure 25: Google retention periods audit logs

Log events name	Lag time
Access Transparency log events	Near real time (couple of minutes)
Admin log events	Near real time (couple of minutes)
Assignments log events	Near real time (couple of minutes)
Calendar log events	Tens of minutes (can also go up to a couple of hours)
Chat log events	1–3 days
Chrome log events	Near real time (couple of minutes)
Classroom log events	1–3 days
Cloud Search log events	Up to a few hours
Context Aware Access log events	Near real time (couple of minutes)
Currents log events	1–3 days
Devices log events	Near real time (couple of minutes)
Directory Sync log events	Near real time (couple of minutes)
Drive log events	Near real time (couple of minutes)
Gmail log events	Near real time (couple of minutes)
Groups log events	Tens of minutes (can also go up to a couple of hours)
Jamboard log events	Near real time (couple of minutes)
Keep	Near real time (couple of minutes)
LDAP log events	Near real time (couple of minutes)
Looker Studio log events	Near real time (couple of minutes)
Meet log events	Near real time (couple of minutes)
Meet quality	Near real time (couple of minutes)
OAuth	Up to a few hours
Rules log events	Near real time
SAML log events	Up to a few hours
Takeout log events	Event when Takeout process starts: Near real time Event when the Takeout process finishes: Depends on the size of the data, up to many days
Tasks log events	Near real time (couple of minutes)
Token log events	A couple of hours
User log events	Login events: Up to a few hours User account events: Tens of minutes
Voice log events	Near real time

Google has made another improvement with regard to the audit logs: the ability for administrators to more easily store and search audit logs in a private data space at Google Cloud via the BigQuery export tool.

Google does not offer a standard option to export log data from one individual via the Domain Wide Takeout tool, only for the organisation or groups within the organisation. When system administrators receive a Data Subject Access Request from a student or employee, they have to export all audit logs and search them for data on one person. Selecting the audit log data relating to 1 specific individual is much easier with BigQuery.

Figure 26: Screenshot of (switching on) BigQuery export

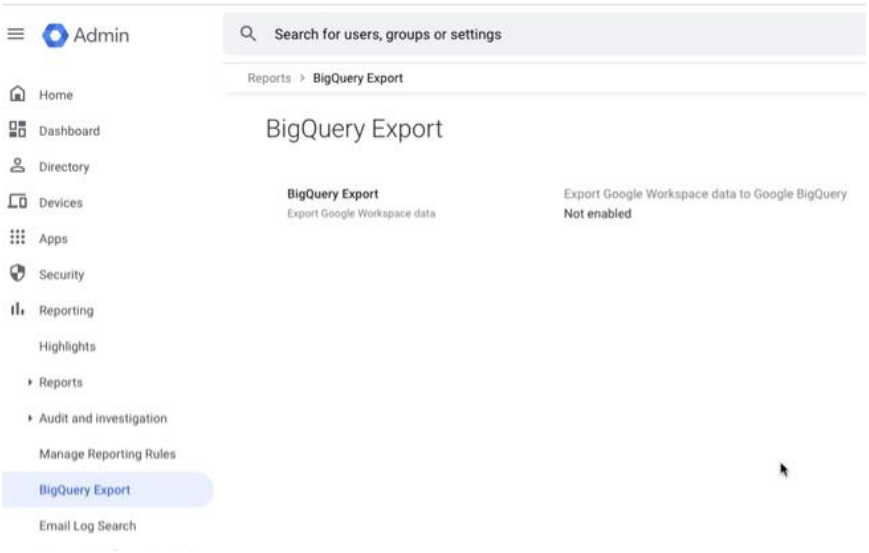
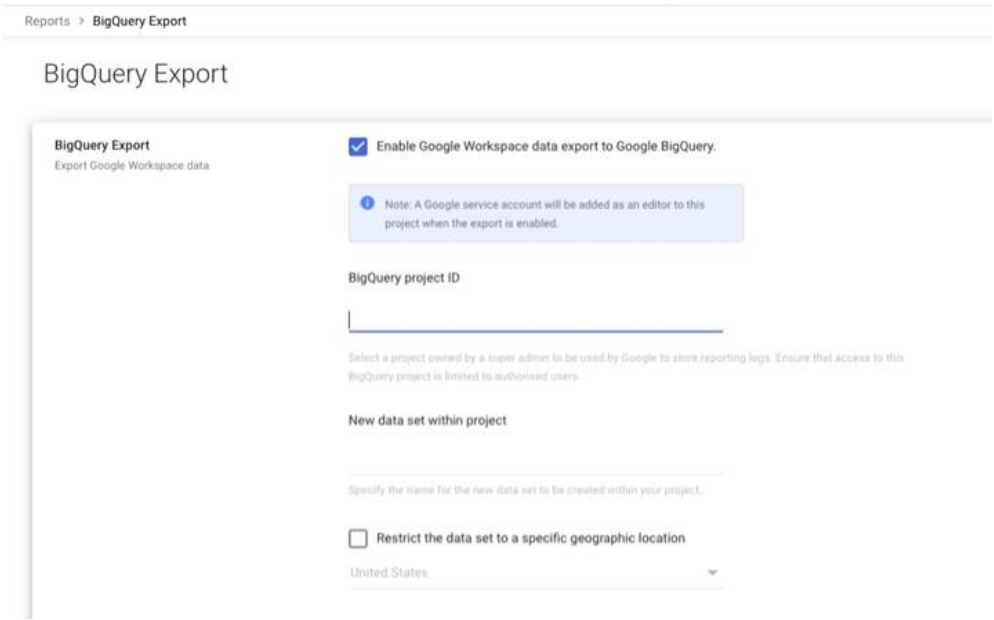


Figure 27: Screenshot of switching on BigQuery export



BigQuery is Google's database (hosted MySQL). To enable BigQuery, the administrator must first enable the *Additional Service* 'Google Developers'. Since Google is a data controller for the Workspace *Additional Services*, the BigQuery data processing would be outside of the agreed Privacy Amendment. However, Google has mitigated this risk by ensuring that an admin needs to click & accept the Google Cloud Platform Terms of Service (which incorporate the Cloud Data Processing Addendum) before the admin is able to use the GCP service BigQuery for the first time. As explained above, all data stored by customers on the cloud platform are Content Data for Google. The Cloud Data Processing Addendum clarifies that Google will process these Content Data as processor for the purposes included in its own global Cloud Data Processing Addendum.

Figure 28: Google Cloud Terms for export of audit logs[39]

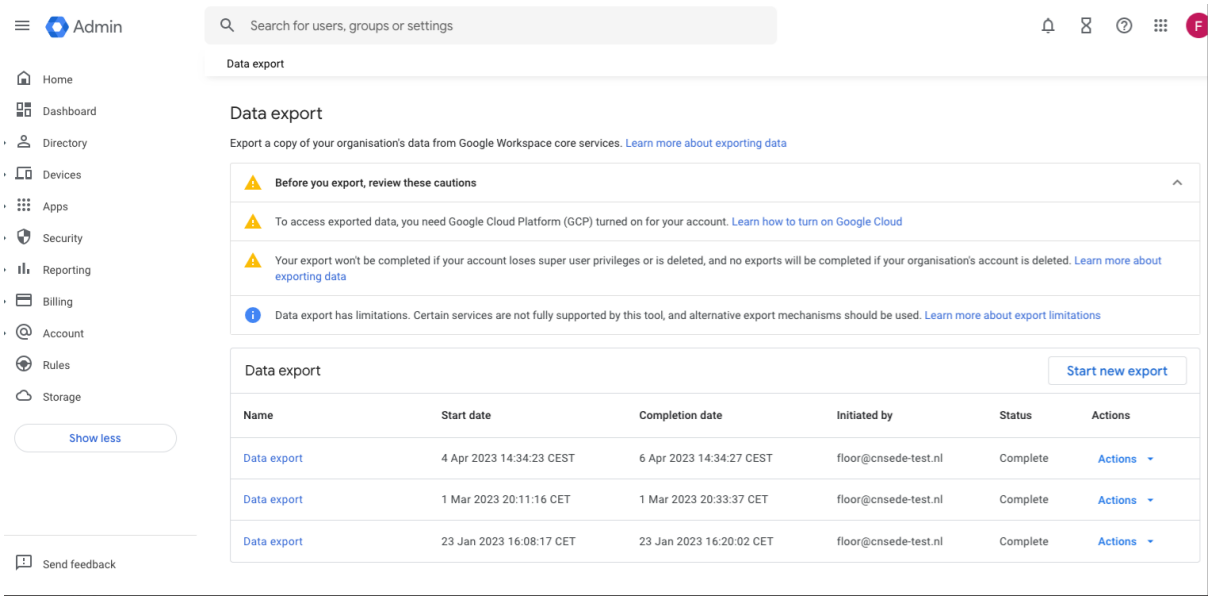
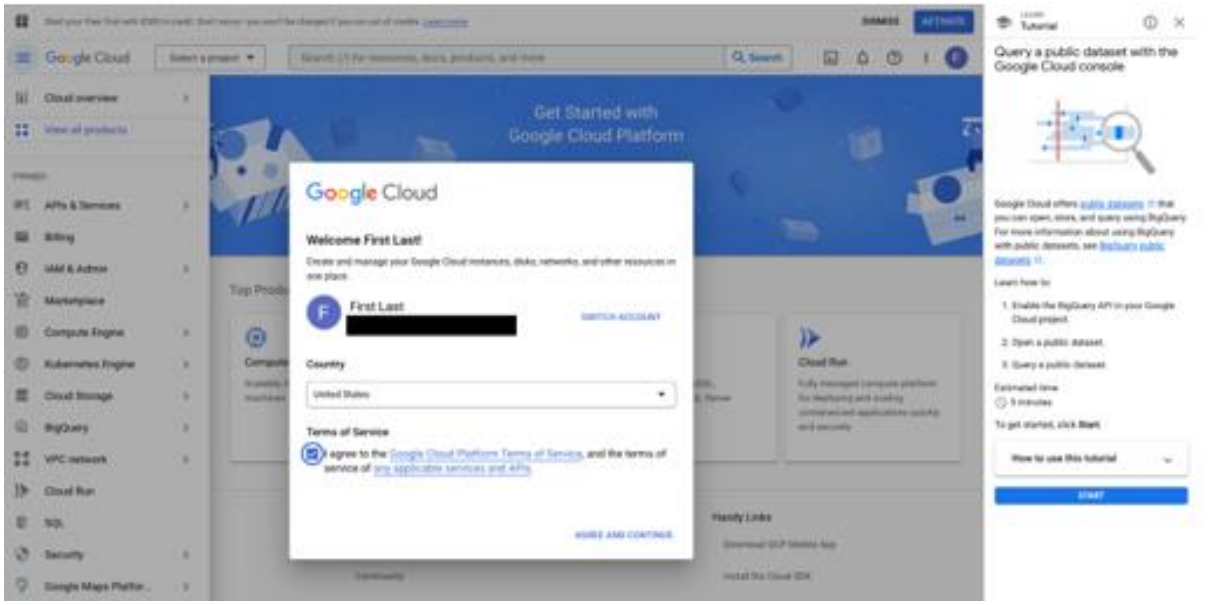


Figure 29: Acceptance Google Cloud Platform (processor) terms for BigQuery[40]



4. Domain Wide Takeout tool for admins to answer data subjects access requests

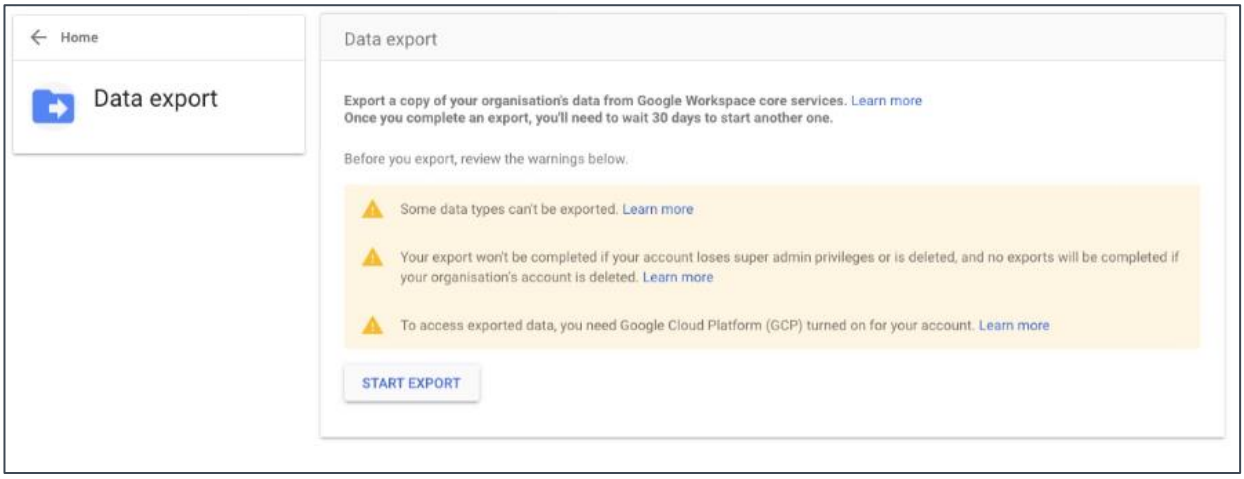
The fourth measure is the Domain Wide Take Out Tool, which allows administrators to export Content Data from a group, faculty or from the entire organisation. Google also offers administrators the ability to enable individual Take Out for end users, allowing them to download their own Content Data from Drive, Gmail, Calendar and Contacts. Both tools do not provide access to log data.

In the test in the K-12 domain with Google Workspace for Education Plus, three things went wrong: firstly, the administrator had to turn on the *Additional Service* Google Cloud Platform for the Domain Wide Take Out tools, secondly, the data export did not seem to work for students in K-12,

[39] Screenshot from the CNS-ede test environment, 12 June 2023. Admins are directed to visit the URL https://console.cloud.google.com/ to accept the Google Cloud Platform terms.
[40] Screenshot provided by Google, 9 June 2023.

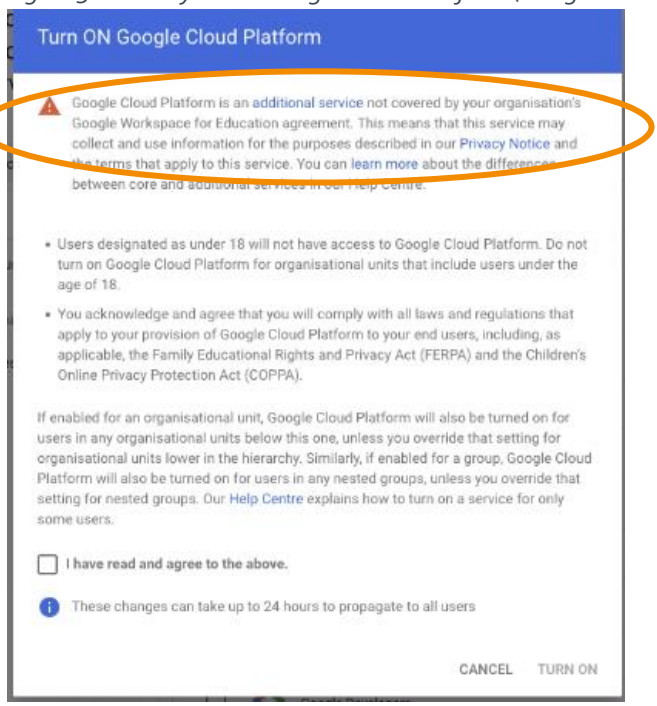
and thirdly, the Take Out Tool did not work in environments with more than 1,000 accounts, as the Rijksuniversiteit Groningen has.

Figure 30: Mandatory use of Google Cloud Platform for data export



Privacy Company was logged in as an administrator in the K-12 environment, but initially did not succeed in exporting the data. Google later explained that the age of the admin had to be changed. If an organisation is qualified as K-12, the age of the administrators is also automatically assigned as under 18 years. This prevents admins from exercising certain rights, such as data export. Google refers to a help article how to create (groups of) admins.[41] Google has also updated the page "*Control access to Google services by age*" to include the words "(including an administrator)" in the section *'Customize the setting for your organization'*.[42] With this explanation, Privacy Company succeeded in exporting the data.

Figure 31: Privacy terms Google Cloud Platform (Google as controller instead of processor)



[41] Google, Get started managing groups for an organization, URL: https://support.google.com/a/answer/33329#configuration .
[42] Google, Control access to Google services by age, URL: https://support.google.com/a/answer/10651918 .

The Domain Wide Data export is not easy to find in the central Admin console. Access is not in the menu, but in a pop-up on the right.

Figure 32: Access to Data Export in administrator console

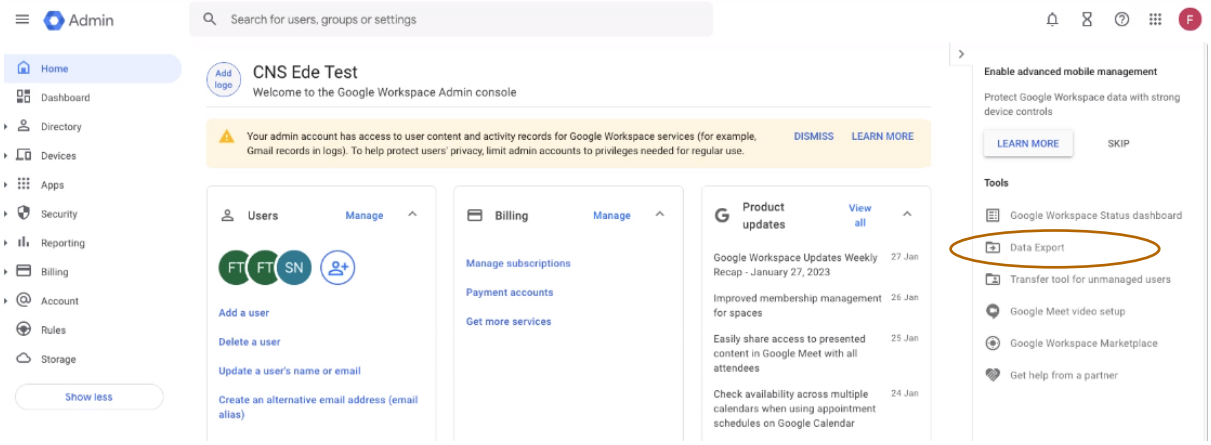


Figure 33: Data export menu administrator

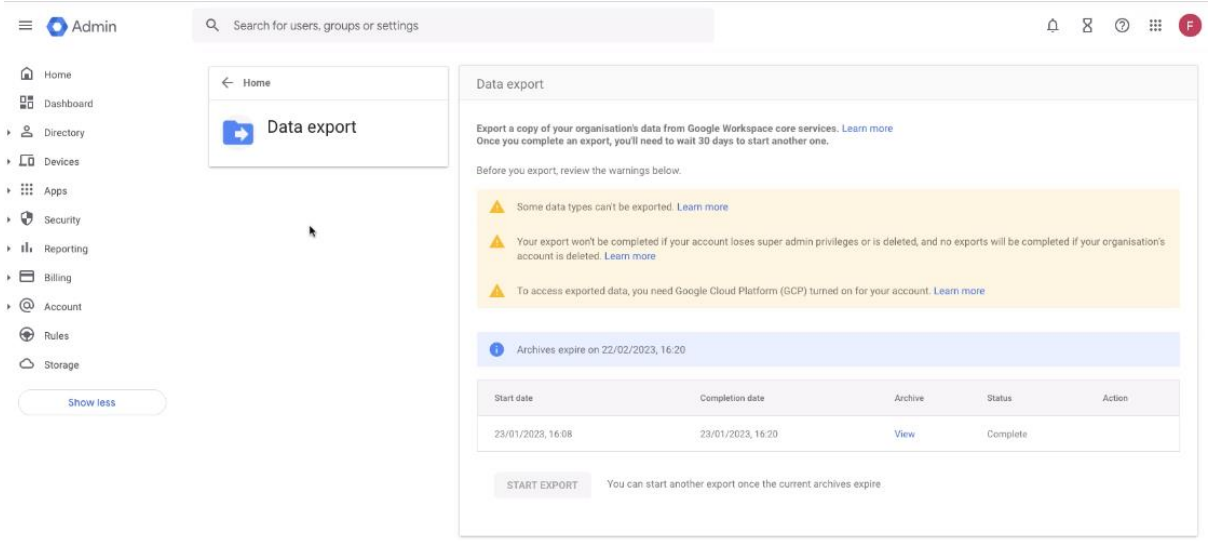
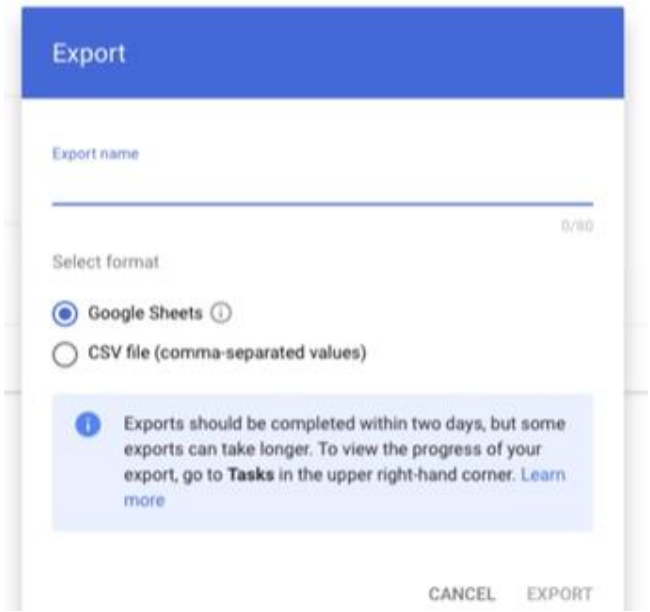
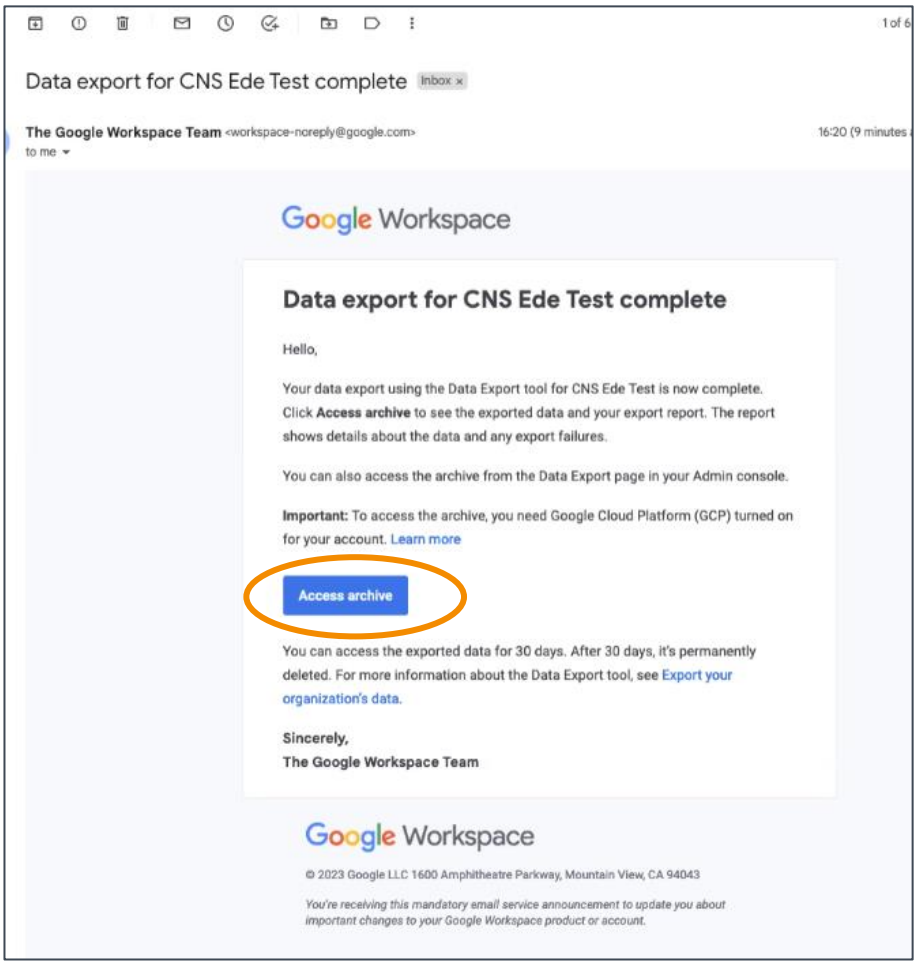


Figure 34: Export menu for administrators



After the administrator determines the form of the export, Google emails when the results are available. In the tiny test environment, the export was ready within a few minutes. See Figure 35 below. It may take longer if there are more users of this tool, or if the tool is used in a larger *tenant*.

Figure 35: Email notification to administrator that the organisation's exported data is available



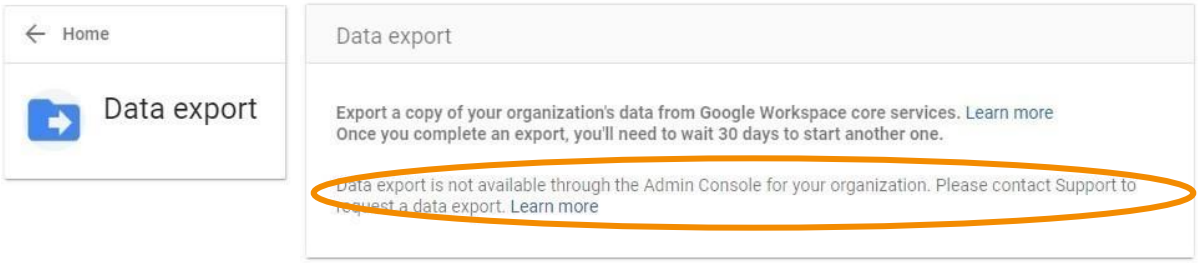
In the university's Workspace for Education environment, the Domain Wide Data Export did not work because the university has more than 1,000 Google accounts. Google explained in the error message that administrators in that kind of large environment should contact Google Support. "*Your organisation should not have more than 1,000 users. If you have more than 1,000 users, you can request temporary access to the Data Export tool by contacting Google Workspace support.*"[43] See Figure 36 below.

In reply to questions from SURF and SIVON about the data protection guarantees for these data when Google Support accesses these data, Google has updated its public documentation, including the guarantee:

> *"The Google Workspace support team does not access or process the data that will be exported via the Data Export tool."*[44]

[43] Google, Export all your organization's data, URL: https://support.google.com/a/answer/100458?hl=en
[44] Idem.

Figure 36: Screenshot of the error message in the administrator interface data export at the university



In both the K-12 test environment and the university environment, the administrator was able to enable the individual Takeout. The results of this individual TakeOut are discussed under the eighth risk (data subject access rights).

In the documentation about Domain Wide Takeout, Google uses the term 'administrator groups'. Google explained that this means that controls do not have to be applied by the super admin but can be applied at group level.

In sum, the Data Export contributes to the mitigation of the high risk of lack of data subject access. If admins in K-12 environments set their own age to 18 years, they can store the exported data in the Google Cloud, and query the export with BigQuery without risking further processing by Google of these Content Data for its own purposes as data controller. For tenants with +1.0000 licenses it is important that Google guarantees that assistance from support employees does not change the processor role of Google. This is important because of the unclarity about Google's double role and hence, two lists of permitted purposes for the processing of Support Data. Based on the Privacy Amendment TSS is a processor activity, but Google is also permitted to further process Support Data in support tickets and support requests as controller, for its own legitimate business purposes.

5. Exhaustive list of sub-processors with their subsidiaries, and Google affiliates

The fifth agreed measure was the commitment to provide a limitative list of sub-processors and affiliates to the Dutch schools and universities, with details about their access to the personal data from schools and universities. Google publishes a public version of that list[45] and will make the new version (with information about Service Data processing) available to Dutch schools and universities. Both lists distinguishes between (i) external companies and their affiliates, and (ii) Google affiliates, and describe their activities, such as technical support or maintenance. Both lists include (the same) sub-processors, including those in third countries. The risks of transfer are out of scope of this verification report, and are separately assessed in the ongoing DTIA.

Google explains that the subprocessors that provide technical support do not have access to Content Data unless the customer knowingly grants access to data stored in their own environment:

> *"These Subprocessors do not have access to Customer Data stored or processed by the Services. They only have access to Customer Data if Customer explicitly elects to enable such access in the course of a support case (e.g., by granting access to a Google Doc, Google Sheet, or Google Drive folder)."*[46]

Google explains that the second list of companies, which are part of the Google group, can process personal data for three types of work:

1. *Data Center Operations: Operates and maintains the Google data center and equipment that stores Customer Data. Subprocessor personnel do not require access to Customer Data to perform this activity.*

[45] Google Workspace and Cloud Identity Subprocessors, Last updated: 18 August 2022, URL: https://workspace.google.com/terms/subprocessors.html.
[46] Idem.

2. *Service Maintenance: Software and systems engineering, maintenance and troubleshooting. In the course of performing this activity the Subprocessor may require limited, authorized access to Customer Data e.g. to remediate technical issues.*

3. *Technical Support: Customer-initiated technical support: (…) In the course of performing this activity, the Subprocessor may require limited, authorized access to Customer Data to respond to Customer-initiated requests."*[47]

In the new list for Dutch schools and universities, Google provides an extra explanation about the purposes for which its subprocessors and affiliates may process the Service Data for support purposes:

- *triage Customer's request and assign relevant personnel. For example, to perform this activity, the Subprocessor will process Customer's designated priority level for the request and information provided by the Customer about the issue specified in the request.*

- *diagnose and investigate the issue specified in the Customer's request (including, as appropriate, attempting to reproduce the issue and/or troubleshooting the issue with Customer), and identify potential ways to address it. For example, to perform this activity, the Subprocessor may need to process error logs impacting Customer's projects, account or environment, or Customer's settings and configurations for the Services.*[48]

Google also provides an extra explanation about access to Service Data for Service Maintenance purposes:

> *"In the course of performing this activity, the Subprocessor may require limited, authorized access to Service Data to identify, address and fix security threats, and to remediate technical issues. For example, the Subprocessor may process:*
>
> - *Aggregated Service usage log data to assess the operational status of the Services for Customer and detect anomalies.*
>
> - *Aggregated diagnostic information to identify technical issues that may occur, such as application crashes."*[49]

With these extra explanations, Google has complied with the fifth agreed measure to mitigate the fourth high risk. With the publication of this list of subprocessors, Google has also mitigated the seventh high risk (see below).

The sixth and seventh agreed measures are discussed under High risk 3.

Conclusion: fourth high risk mitigated

Google has mitigated the high risk of lack of transparency of the Diagnostic Data by a number of measures. Google has developed a tool to view the last 24 hours of Telemetry Data as well as a process for super admins to access historical Telemetry Data, expanded the admin access to Diagnostic Data via audit logs and ensured admins can securely export data from the Domain Wide Takeout tool to Google Cloud services, including BigQuery, with Google in a processor role (not as controller for an *Additional Service*). On 9 June 2023 Google has also completed the agreed measure to publish adequate documentation about the Telemetry Data and updated its documentation about its sub-processors and subsidiaries.

---

[47] Idem.
[48] Specific subprocessor page provided by Google to SURF and SIVON. soon to be published.
[49] Idem.

High risk 5: Lack of legal ground

This risk originated from Google's role as controller, and had three components:

1. Additional Services
2. Support tickets
3. Reading of non-necessary data from end user devices (cookies and Telemetry Data)

1. Additional Services

The first part of this risk was about the legal ground for Google's own purposes as a data controller for the processing of personal data of pupils and students through *Additional Services* such as YouTube and Search.

In the K-12 environment, access to all *Additional Services* (where Google is the data controller) is blocked by default. This is important, because YouTube is used in many schools to view teaching materials, from their own teachers and from other teachers. It is also a fact that Google Search has a huge market share in the general search engine market. It is therefore plausible that most pupils and students (want to) use this service on a daily basis. Therefore, there will be great pressure on system administrators to enable access to these *Additional Services*.

Contractually, Google is prohibited from relying on consent from the students. Google agrees contractually that end user consent is not applicable as ground for sharing Service Data with third parties when those parties' services are disabled by Customer (including Google as third party for *Additional Services*).

If admins enable access to YouTube, contrary to the advice from SIVON, Google does set restrictions to YouTube use for K-12 users.[50] SIVON recommends teachers to upload videos in the processor service Classroom in the embedded mode. Google recommends linking via Google Drive.[51]

Schools and universities should instruct students and teachers to pay attention to the profile icon in the top right corner of the screen. As soon as that profile icon disappears, the negotiated privacy protections no longer apply. Additionally, system administrators should tell end users not to set Google Search as the default search engine in their browser of users, and to only visit YouTube in the browser's incognito or private mode.

2. Support tickets

The second part of this risk, about Google's role for support tickets with attachments, can also be mitigated by the schools. Based on the Privacy Amendment, Google has become a processor for the Technical Support Services, and thus also for Content Data, if a school decides to actively provide access to support personnel.

As mentioned above in Section 4.4, there is still some unclarity about the further processing by Google in a role as data controller of personal data in support tickets and support requests for Google's legitimate business purposes. As long as schools do not upload personal data in attachments with support requests, they can mitigate this risk.

3. Reading of non-necessary data from end user devices (cookies and Telemetry Data)

The third risk relates to the legal consent requirement for cookies and Telemetry Data. Under statutory law, Google has to comply with the locally implemented rules from the ePrivacy Directive.

---

[50] Google, Understand changes to school accounts on YouTube, URL: https://support.google.com/youtube/answer/10977326?hl=en.

[51] See the SIVON advice (in Dutch only) at https://sivon.nl/update-google-workspace-for-education/. Google also explains this in the Support article, How do I upload a video to Google Classroom, URL: https://support.google.com/edu/classroom/thread/82076531/how-do-i-upload-a-video-to-google-classroom?hl=en.

This means that Google must seek consent for non-functional cookies and other information it reads from the end user's device. While most of the Telemetry Data Privacy Company has seen through the DIT contains information that may fall under the specific Dutch exception for analytical information, the appearance of Content Data in events related to the Grammar and spell check appeared to require consent. As explained in the section about the fourth high risk, and shown in Figure 20 above, Google has convincingly explained why this data collection is strictly necessary for the functioning of the requested Spelling and grammar check service, as the entire processing takes place in the browser on the end user device, and Google has no other way of collecting information about the accuracy of the service. Google has also explained it applies the shortest retention period of 30 days to these Content Data.

Conclusion: fifth high risk mitigated

Google has mitigated all three identified components of the fifth high risk through a combination of contractual and technical measures.

High risk 6: Missing privacy controls

Google has taken the three agreed mitigation measures to mitigate the sixth high risk.

1. Administrators can centrally prohibit the use of Additional Services with a Workspace for Education account (already disabled by default in K-12)
2. Google has changed the default ads personalisation setting for new Workspace for Education users: it is now off by default.
3. While there is no way for administrators to centrally disable Workspace Spelling and grammar check, Google has committed not to reuse content from the Spelling and grammar check outside the tenant. This is not explicitly stated in the Workspace for Education (online) agreement, but it is in two of Google's public documents: the Workspace for Education Data Protection Implementation Guide and the Security whitepaper. Because Google makes these public commitments, Google is also beholden to comply with these promises under Section 5 of the FTC Act.[52]

Conclusion: sixth high risk mitigated

Google has mitigated the three components of the sixth high risk through technical and contractual measures.

In Table 1 in this report, the fifth and sixth risk have been merged.

High risk 7: Lack of control sub-processors and affiliates

As explained under the fourth high risk, Google publishes an exhaustive list of sub-processors with their affiliates, and subsidiaries (members of the Google group). For the Dutch schools and universities, the list has been supplemented with additional information about the access from these parties to Service Data.

While the subprocessors listed in each resource are exactly the same, the resources are different in that Google normally does not process the Service Data as processor. Hence in its global communication Google cannot call the companies it engages for support and maintenance "sub-processors" to the extent they process Service Data. The list for the Dutch schools and universities begins with the following:

[52] FTC, A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority, URL: https://www.ftc.gov/about-ftc/mission/enforcement-authority.

"This webpage only applies where, under the applicable agreement for the Google Workspace and Cloud Identity Services, Customer has elected to instruct Google to process Service Data as a processor. In all other cases, the information about Subprocessors for Google Workspace and Cloud Identity Services is available at https://workspace.google.com/terms/subprocessors.html."

Google has ensured that all subprocessors, including their affiliates, and Google's subsidiaries are bound by Google's contractual arrangements with schools and universities. This includes use of the SCC.

*[**Confidential**]"*[53]

Under the Privacy Amendment, schools and universities [**confidential**].

Google has clarified that sub-processors and subsidiaries that are given access to Content Data (Customer Data) also have access to Service Data. Google describes in its public documentation (the list of sub-processors) that staff at sub-processors can only access Content Data if the customer gives permission, for example by granting access to a Google Drive folder.[54] This limited access for support purposes (only in reply to a request from a customer) also applies to subsidiaries:

"In the course of performing this activity, the Subprocessor may require limited, authorized access to Customer Data to respond to Customer-initiated requests".

Google has also explained the limitations of access to Service Data. For support issues, employees can access error logs impacting Customer's projects, account or environment, or Customer's settings and configurations for the Services, but only in reply to a reported problem. With regard to maintenance, generally staff only gains access to aggregated data.

Conclusion: seventh high risk mitigated or out of scope

Google has expanded its documentation about its sub-processors and subsidiaries, which mitigates the high risk. The risks of transfers of personal data to subprocessors and subsidiaries in third countries are out of scope of this report, and are being addressed in the ongoing DTIA.

High risk 8: Lack of data subject access to personal data

The Update DPIA identified a high risk relating to (a lack of) data subject access, in particular to the Diagnostic Data (including Telemetry Data, data from Google's security logs and data related to webserver access logs and cookies). In reply, Google referred to

1. Existing self-service tools for end-users
2. New access tools for admins
3. Google's own Data Subject Access Request form, and
4. A new explanation with legitimate reasons to refuse access to some personal data.

---

[53] **Confidential** SURF and SIVON Privacy Amendment with Google.
[54] Google Workspace and Cloud Identity Subprocessors, URL: https://workspace.google.com/terms/subprocessors.html Google explains: "*They only have access to Customer Data if Customer explicitly elects to enable such access in the course of a support case (e.g., by granting access to a Google Doc, Google Sheet, or Google Drive folder).*"

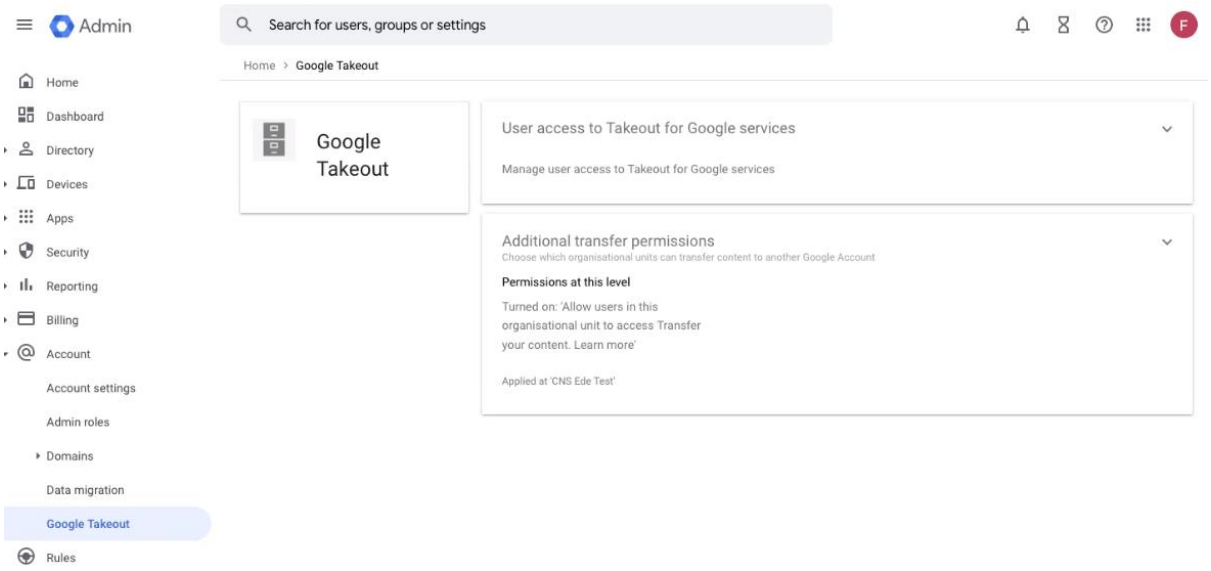
1. Self-service tools for end users

Google describes in its Workspace Data Subjects Requests Guide that users have access to several self-service tools to download their data, and can ask admins for an export of data.[55] Google also provides a help center article with hyperlinks.[56]

2. Access tools for admins

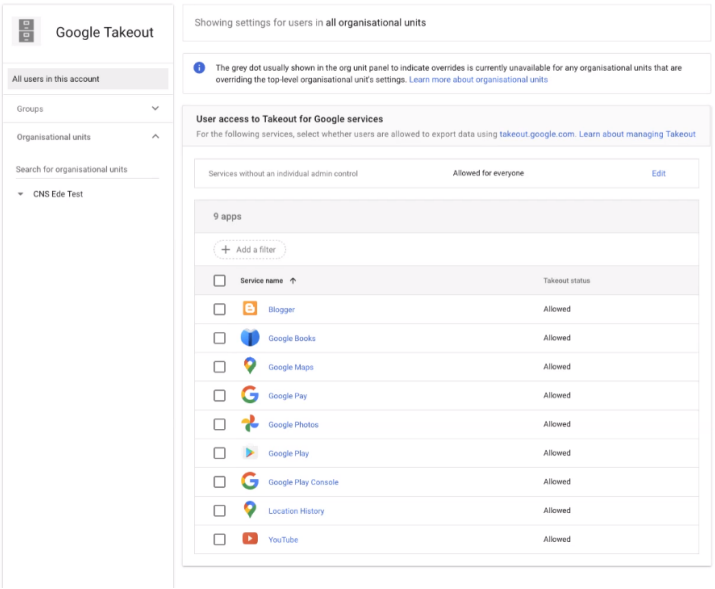
Google has developed an individual TakeOut tool that administrators of Workspace for Education environments can enable. As shown in Figure 37 below, the admin can give users permission to takeout their own personal data.

Figure 37: Screenshot administrator interface university for individual Takeout Gmail and Drive files



The administrator can also authorise users to export data from some specific *Additional Services*: but these should be or are by default disabled (in K-12).

Figure 38: Export of Content Data from Additional Services



[55] Google Workspace Data Subject Requests (DSR) Guide, last updated February 2022, URL: https://services.google.com/fh/files/misc/gsuite_dsr_customer_guide.pdf.
[56] Google Privacy Help Center, URL: https://support.google.com/policies/answer/9581826?hl=en.

Privacy Company tested the individual export in the K-12 test environment, via https://takeout.google.com. Users can also export limited individual log activity data via this tool. The export is limited to the same data that are also available via https://myactivity.google.com/myactivity

Figure 39: Screenshot of individual TakeOut: choice of log files

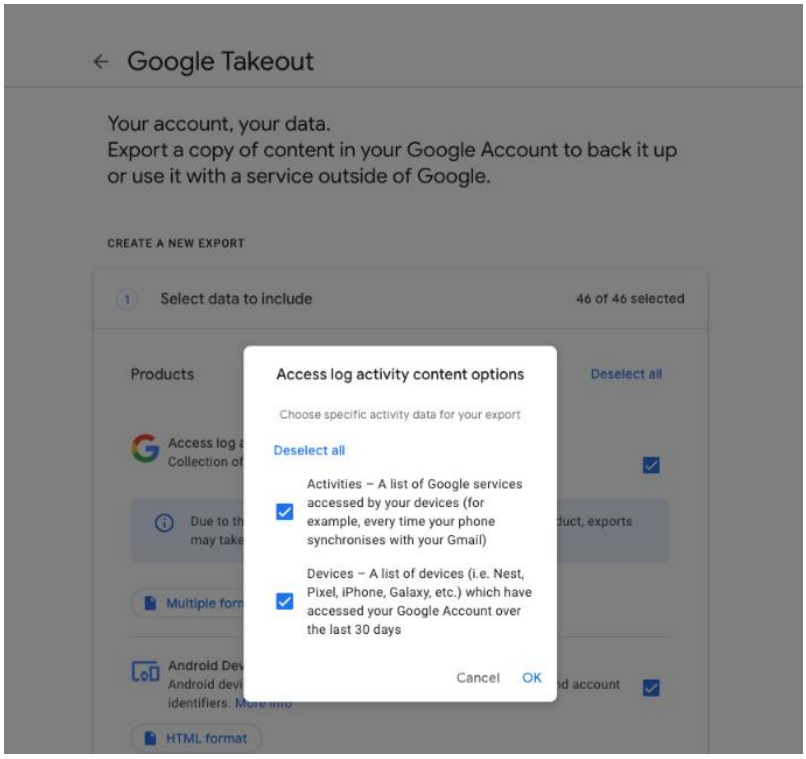


Figure 40: Screenshot of individual TakeOut: choice for additional information about Drive files

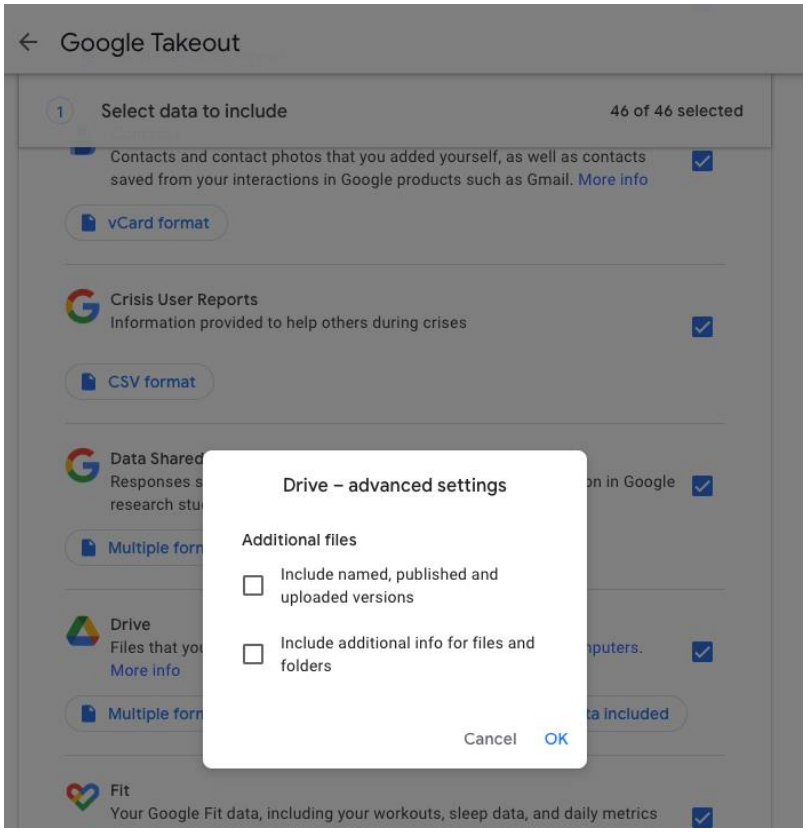
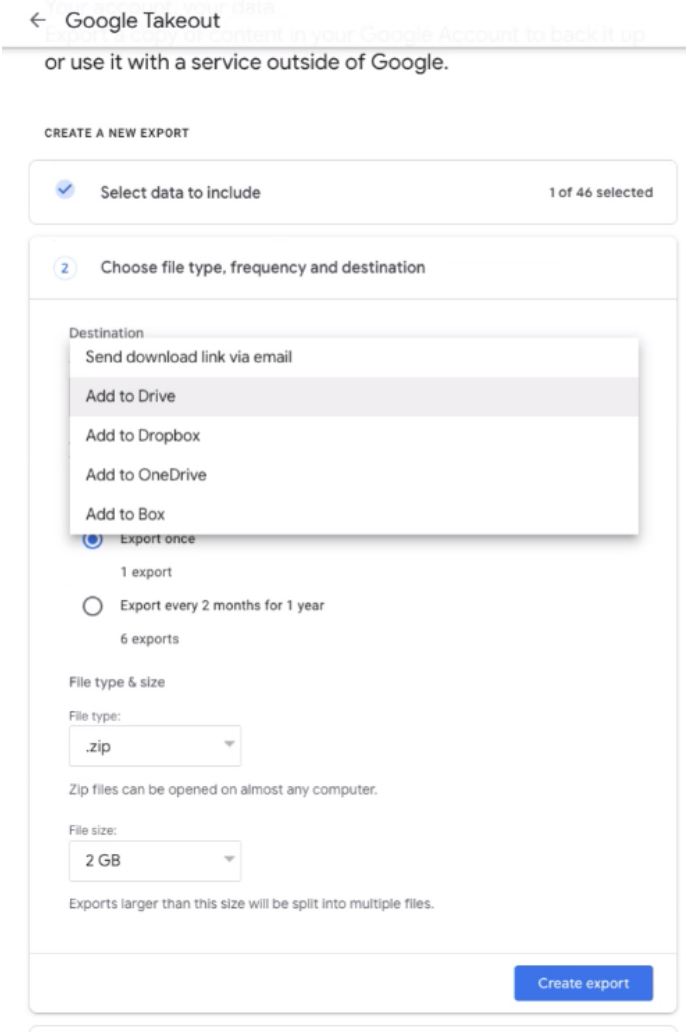
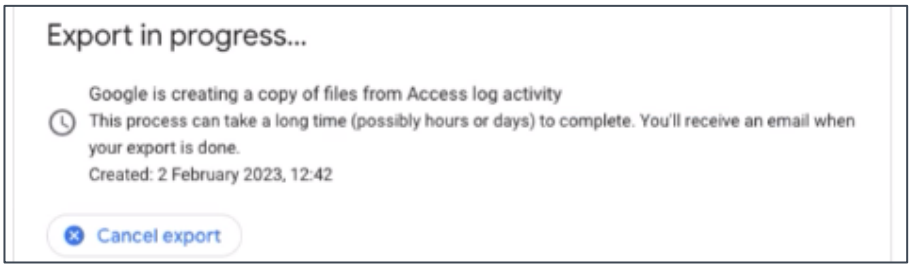


Figure 41: User choices for export of individual TakeOut data



Google explains that exporting the individual logs can take hours or days.

Figure 42: Screenshot data export in progress



The exported activity logs are also available via the Google Account Dashboard and Activity Dashboard. These logs provide insight into which Google services a user has used recently, and for example, who viewed a shared file when, but no detailed log data.

Figure 43: Screenshot activity logs via Google Dashboard

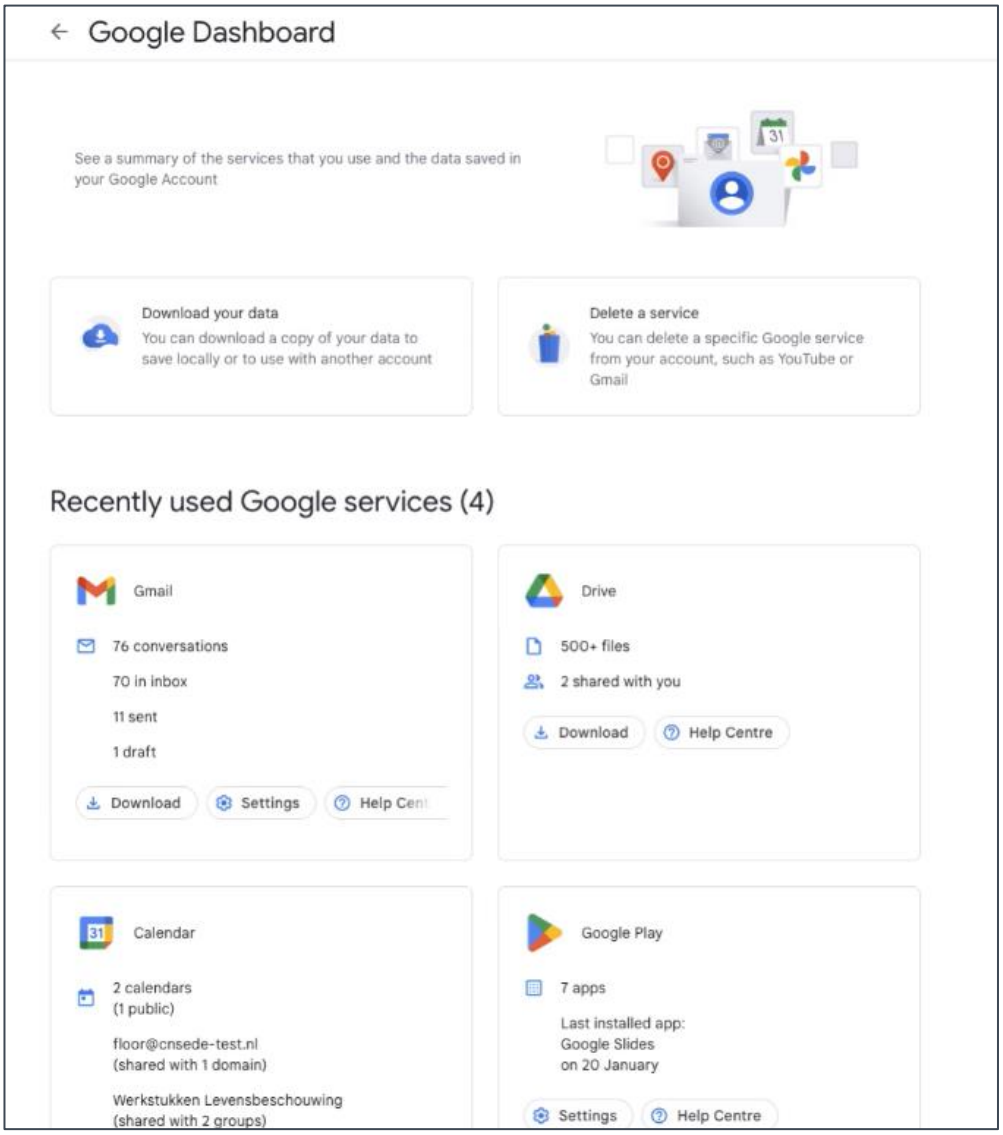
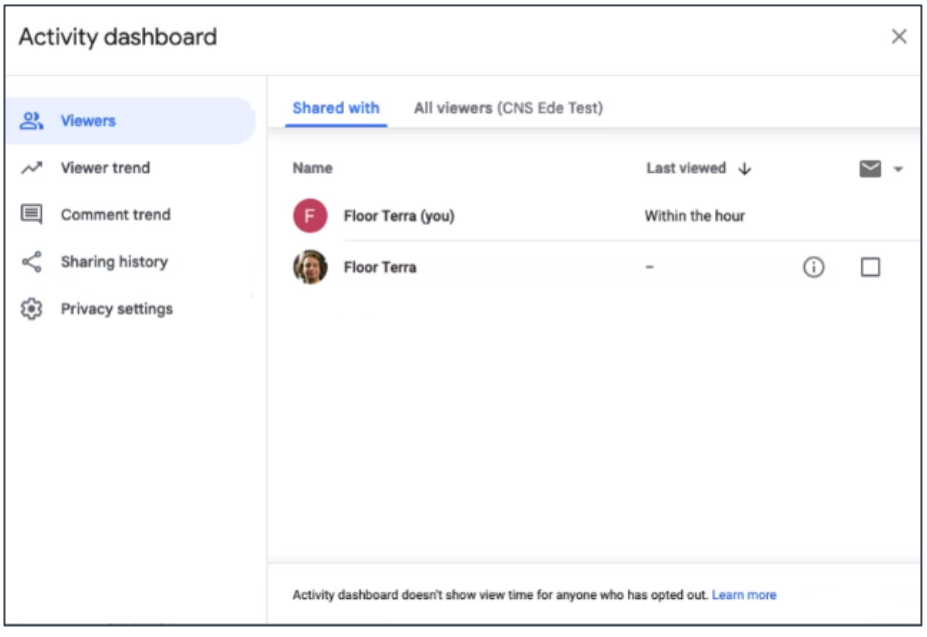


Figure 44: Screenshot detail information in Activity Dashboard



Though the individual Takeout tool is a very helpful tool for end users to obtain access to their Content Data, and to gain some insights in the types of activities processed by Google, the tool does not provide access to the Diagnostic and Telemetry Data processed by Google.

As described above, under High risk 4, Google has developed the Diagnostic Information Tool and a manual process for super admins to obtain access to Telemetry Data. Google has also expanded the availability of audit logs for admins, which they can export to query for individual log data.

The only other personal Diagnostic Data that were missing in reply to the Data Subject Access Request filed by Privacy Company as end user in the K-12 test environment were personal data relating to Google's security logs, and personal data relating to webserver access logs and cookies. Google's reasons to refuse access to these data are discussed below under 4).

3. Google's DSAR form

To complete the list of tools to obtain access to personal data, Google has a DSAR form. [57] Users can use this form when Google processes data as data controller (including the 7 agreed Legitimate Business Purposes). This form is not very user friendly. A user must (still) type in their own description of data categories, rather than being able to select categories from a drop-down menu. Users cannot be expected to know or accurately describe the available data categories.

Therefore, schools and universities are advised to provide guidance to students and employees about the different tools to access personal data, and how to use the DSAR form.

Table 4: Overview of data subject access tools

Type of Data Subject Access tool	Output data
Download Content Data by logging in to the Google account	Content Data
My Activity (saved activity)	Activity Data such as browsing history and searches
Download data via individual Google Takeout (if enabled by admin)	Content Data, Account data, Play Store and Access Log Activity, also relating *to Additional Services* when enabled.
Diagnostic Information Tool (via admin)	Telemetry Data limited to the last 24 hours
Organisation Data Export (via admin)	Content and Diagnostic Data
Historical Telemetry Data (via super admin)	All available historical telemetry data, through the super admin of the organisation
Google Data Access Form	Request all available personal Google processes as data controller in relation to the Workspace for Education account, except for the Content Data and activity logs that the user can download via the self-service tools.

Google has committed to provide an individual answer if an end user uses the DSAR form, even though it explains it will automatically reply with a reference to the self-service tools in its first response, while it is still querying for specific data.

Google has also committed to inform end users and provide access to an appeal procedure if they are flagged in a copyright complaint or, for example, a CSAM filter, unless legally prohibited.

[57] Access via Google after log-in, URL: https://support.google.com/policies/contact/sar?hl=en

4. Google's reasons to refuse access

Google has updated its information page with general explanations on reasons why it does not provide access.[58] 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)[59]

The reason Google does not provide separate access to logged data about cookies (in webserver access logs) 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."*[60].

Google explains that it does not categorically refuse access to personal data. This applies to both webserver/cookie data and Security Data as many of these data, such as device fingerprints and IP addresses, are available in other copies of the data, used for other purposes, such as Telemetry Data.

With regard to Security Data, 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."*[61]

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 known, it could give potential bad actors valuable signals that could be used to exploit our systems."*[62]

Privacy Company did not perform a retest of filing a data subject access request. As established in the Update DPIA report, it is up to the supervisory authority, the Dutch Data Protection Authority,

---

[58] Google, Information not provided in response to an access request, URL: https://support.google.com/policies/answer/10972441.
[59] Idem.
[60] Google Privacy Help Center, URL: https://support.google.com/policies/answer/9581826?hl=en, under 'Can I use other information related to or from a Google account to access data associated with that Google account?'
[61] Google, Information not provided in response to an access request.
[62] Idem.

to assess whether Google (in its role as data controller) complies with the requirements of the GDPR in reply to data subject access requests, if a user complains that the access would be insufficient.

Conclusion: eighth high risk mitigated

Google's different access tools provide access to many personal data. Google allows end users to download many data via self-service tools, and has taken measures to allow admins much more access to, and export of, the Diagnostic Data available in audit logs. These measures mitigate the high risk of a lack of data subject access when Google acts as processor.

As data controller (for the agreed 7 legitimate business purposes, and for the *Additional Services*) Google has provided an expanded explanation of possible refusal reasons, and has committed to provide an individual answer to each request filed through its controller DSAR form. As established in the Update DPIA report, it is up to the Dutch Data Protection Authority, when a complaint is filed to assess whether Google (as a controller) complies with the requirements of the GDPR.

High risk 9: Transfer to third countries [out of scope]

SURF and SIVON are currently analysing the transfer risks in a separate project with Google, together with the procurement officers of the central Dutch government (*SLM Microsoft, Google and Amazon Web Services Rijk*[63]) in the context of a Data Transfer Impact Assessment (DTIA).

[63] SLM Microsoft, Google Cloud en Amazon Web Services, URL: https://slmmicrosoftrijk.nl/.

http://www.privacycompany.eu/
info@privacycompany.nl

Annex

Two examples of telemetry messages with Content Data

In these two messages resulting from the use of Google Meet, directly identifiable data are highlighted in yellow.

SOURCE: export Diagnostic Information Tool, payload exported as Meet.csv

2023-01-20T16:21:49.563865+01:00,45.137.101.242INbQvqvlz_HlSw, "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:107.0) Gecko/20100101 Firefox/107.0,gzip(gfe)","{""common_event_logging"":""client_info { client_type: JS browser_info { locale: \"en-US" browser: \"Firefox" browser_version: \"107.0" } js_client_info { os_type: MAC os_version: \"10.15" device_type: DESKTOP locale: \"en-GB" build_label: \} } log_source: **HANGOUT_LOG_REQUEST** timestamp_millis: 1674228106535 client_timestamp_millis: 1674228106414 event_code: 3406"",""http_lang"":""en-US,en;q=0.5""",""meet_logging"":""log_entry { hangout_identifier { resource_id: \""boq_hlaneBECB648D\"" session_id: \"qNoHp3tYUKMsgwoKAAiKAiADEA"" hangout_id: \"G1PcA-Tms_g5924PyB1uDxIMOAIoABgCEAgIigIgAwg"" participant_id: \""spaces/aK8yOVn2p70B/devices/5147c04f-a791-4bee-8af1-9f9f5e11fdb7\"" participant_log_id: \""boq_hlane_2SaK6SQ52pf\"" user_jid: \"floor@cnsede-test.nl" meeting_code: \"sra-dyib-eqs" meeting_space_id: \} system_info_log_entry { appVersion: \} impression_entry { type: 3406 additional_data { str_value: \} } hangout_client_info { property_name: \""""boq_hlane"" } } rtc_client { device: DESKTOP application: BOQ_HOTLANE platform: WEB host_environment: STANDALONE hub_configuration: MEET_CONFIGURATION media_participation_mode: MEDIA_PARTICIPATION_CALL_PARTICIPANT }""",""visual_elements"":""[]""",""request_context"":""""NULL""}""

2023-01-20T16:21:49.563684+01:00,45.137.101.242,INbQvqvlz_HlSw, "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:107.0) Gecko/20100101 Firefox/107.0,gzip(gfe)","{""common_event_logging"":""client_info { client_type: JS browser_info { locale: \"en-US" browser: \"Firefox" browser_version: \"107.0" } js_client_info { os_type: MAC os_version: \"10.15" device_type: DESKTOP locale: \"en-GB" build_label: \} } log_source: **HANGOUT_LOG_REQUEST** timestamp_millis: 1674228100140 client_timestamp_millis: 1674228100019 event_code: 4764"",""http_lang"":""en-US,en;q=0.5""",""meet_logging"":""log_entry { hangout_identifier { resource_id: \{ "boq_hlaneBECB648D" participant_log_id: \""boq_hlane_2SaK6SQ52pf\"" user_jid: \"floor@cnsede-test.nl" meeting_code: \"sra-dyib-eqs" meeting_space_id: \} system_info_log_entry { appVersion: \} impression_entry { type: 4764 additional_data { str_value: \"Mic: FloorPixel Buds Pro ofsEf9xsW1cc3MpuBpbcqPCFn//OjDHP88JaR5u7zok=, Speaker: System default speaker device __synthetic_default_speaker_device__, MatchableDevice: \"" } } hangout_client_info { property_name: \""""boq_hlane"" } } rtc_client { device: DESKTOP application: BOQ_HOTLANE platform: WEB host_environment: STANDALONE hub_configuration: MEET_CONFIGURATION media_participation_mode: MEDIA_PARTICIPATION_CALL_PARTICIPANT }""",""visual_elements"":""[]""",""request_context"":""""NULL""}""

Example of *Spelling and grammar check*

In this long message, the Content Data collected as a result of the use of the *Spelling and grammar check* are highlighted in yellow (on the next page).

2023-01-20T17:25:51.725166+01:00,

45.137.101.242,

INbQvqvlz_HlSw,

"Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:107.0) Gecko/20100101 Firefox/107.0,gzip(gfe)",

{

"common_event_logging": "client_info {

client_type: JS

browser_info {

locale: "en-US"

browser: "Firefox"

browser_version: "107.0"

}

js_client_info {

os_type: MAC

os_version: "10.15"

device_type: DESKTOP

locale: "en-GB"

}

}

log_source: SLIDES

timestamp_millis: 1674231951721

client_timestamp_millis: 1674231951622

impression_batch {

impressions {

entry_point: CONTEXT_MENU

sequence_number: 159

event_details {

docs_common {

window_size {

inner_width: 1625

inner_height: 1232

outer_width: 1625

outer_height: 1317

}

in_revision_history: false

impression_context: SKETCHY_CURRENT_PAGE

impression_context: SKETCHY_SHAPE

impression_context: SKETCHY_TEXT

action_data {

apply_spellcheck_suggestion_rank: 1

spelling_language: "la"

document_local: "en"

spelling_details {

context: "ididunt ut labore et dolore magna aliqua homework splelling"

suggestion: "spelling"

misspelling_start: 50

misspelling_end: 58

underlines_count: 0

suggestion_type: UNDEFINED_SUGGESTION_TYPE

suggestion_tag: SPELLING

affected_underlines_count: 1

underline_count_by_source_and_tag {

tag: SPELLING

underline_count: 0

affected_underline_count: 1

}

suggestion_model: UNDEFINED

misspelling_fingerprint {

context_simhash: 0

suggestion_hash: 0

}

ui_context: CONTEXT_MENU

}

}

view_mode: FULL_CHROME

has_edited: true

access_state {

is_commentable: true

is_editable: true

}

find_details {

doco_match_selected: false

}

device_pixel_ratio: 1.0

}

connection_details {

connection_status: ONLINE

}

ui_interaction {

pointer_event_type: MOUSE

}

companion_used_in_session: false

}

last_heartbeat_sequence_number: 1

client_timing_info {

elapsed_timing {

start_client_time_usec: 1674231944849000

end_client_time_usec: 167423194489800o

}

timing_type: ELAPSED

}

event_code: 121

start_sequence_number: 159

end_sequence_number: 163

}

impressions {

sequence_number: 126

event_details {

text_modification {

input_method: KEYBOARD

}

}

```
last_heartbeat_sequence_number: 1
high_frequency_details {
num_activity_components: 10
closing_trigger: UNLOAD
}
client_timing_info {
elapsed_timing {
start_client_time_usec: 1674231938011000
end_client_time_usec: 1674231951620000
}
timing_type: ELAPSED
}
event_code: 1313
start_sequence_number: 126
end_sequence_number: 164
}
impressions {
sequence_number: 118
event_details {
ui_interaction {
pointer_event_type: MOUSE
}
canvas_interaction {
un _buckets {
interaction {
 count: 1
 gesture_type: GESTURE_STATIONARY
}
}
}
}
last_heartbeat_sequence_number: 1
high_frequency_details {
num_activity_components: 1
closing_trigger: UNLOAD
```

```
 }
 client_timing_info {
 elapsed_timing {
 start_client_time_usec: 1674231935442000
 end_client_time_usec: 1674231951620000
 }
 timing_type: ELAPSED
 }
 event_code: 29564
 start_sequence_number: 118
 end_sequence_number: 165
}
session_info {
 session_id: "CKnm2PrH1vwCFRSNqwcdC70PeQ"
 client_start_time_usec: 1674231928383000
 server_start_time_usec: 1674231927943983
 session_type: PUNCH_WEB
}
client_info {
 ui_locale: "en-GB"
 user_agent: "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:107.0) Gecko/20100101 Firefox/107.0"
 document_id: "1QQI4oqwLdVx1vZYg6zaEh6_V0ZCk1eN6UE84uKA67No"
 offline {
 is_cold_start: false
 is_opted_in: false
 }
 has_edited: true
 job set: PROD
 experiment {
 experiment_id: 5700019
 experiment_id: 5700036
 experiment_id: 5700057
 experiment_id: 5700103
 experiment_id: 5700114
 experiment_id: 5700133
```

experiment_id: 5700333

experiment_id: 5700884

experiment_id: 5700893

experiment_id: 5701034

experiment_id: 5701641

experiment_id: 5702392

experiment_id: 5702538

experiment_id: 5702785

experiment_id: 5703182

experiment_id: 5703206

experiment_id: 5703307

experiment_id: 5703575

experiment_id: 5703839

experiment_id: 5704387

experiment_id: 5704572

experiment_id: 5704621

experiment_id: 5704883

experiment_id: 5705891

experiment_id: 5706270

experiment_id: 5706523

experiment_id: 5706669

experiment_id: 5706786

experiment_id: 5706999

experiment_id: 5707047

experiment_id: 5707204

experiment_id: 5707327

experiment_id: 5707445

experiment_id: 5707609

experiment_id: 5707695

experiment_id: 5707711

experiment_id: 5707820

experiment_id: 5708235

experiment_id: 5708365

experiment_id: 5708560

experiment_id: 5708886

experiment_id: 5709085

experiment_id: 5709201

experiment_id: 5709209

experiment_id: 5709476

experiment_id: 5709673

experiment_id: 5710189

experiment_id: 5710692

experiment_id: 5711230

experiment_id: 5711550

experiment_id: 5711669

experiment_id: 5712189

experiment_id: 5712489

experiment_id: 5712556

experiment_id: 5712635

experiment_id: 5712909

experiment_id: 5712913

experiment_id: 5713195

experiment_id: 5713554

experiment_id: 5713993

experiment_id: 5714310

experiment_id: 5715322

experiment_id: 5717909

experiment_id: 5719464

experiment_id: 5719484

experiment_id: 5722141

experiment_id: 5722201

experiment_id: 5722802

experiment_id: 5723989

experiment_id: 5724217

experiment_id: 5724437

experiment_id: 5726697

experiment_id: 5727259

experiment_id: 5728004

experiment_id: 5728967

experiment_id: 5730227

experiment_id: 5730287

experiment_id: 5731837

experiment_id: 5732343

experiment_id: 5733770

experiment_id: 5734614

experiment_id: 5735136

experiment_id: 5735254

experiment_id: 5735808

experiment_id: 5736413

experiment_id: 5737256

experiment_id: 5737802

experiment_id: 5739780

experiment_id: 5740188

experiment_id: 5740343

experiment_id: 5740816

experiment_id: 5741976

experiment_id: 5742726

experiment_id: 5743146

experiment_id: 5743789

experiment_id: 5744290

experiment_id: 5744350

experiment_id: 5745460

experiment_id: 5746726

experiment_id: 5746786

experiment_id: 5747218

experiment_id: 5747943

experiment_id: 5749257

experiment_id: 5750112

experiment_id: 5750878

experiment_id: 5750956

experiment_id: 5751159

experiment_id: 5752152

experiment_id: 5752676

experiment_id: 5753663

experiment_id: 5753683

experiment_id: 5754311

experiment_id: 5754830

experiment_id: 5755411

experiment_id: 5756697

experiment_id: 5757324

experiment_id: 5758499

experiment_id: 5758638

experiment_id: 5758676

experiment_id: 5759280

experiment_id: 5759564

experiment_id: 5760169

experiment_id: 5760329

experiment_id: 5760452

experiment_id: 5760472

experiment_id: 5762731

experiment_id: 5763275

experiment_id: 5763519

experiment_id: 5764067

experiment_id: 5764468

experiment_id: 5768934

experiment_id: 5770337

experiment_id: 5771105

experiment_id: 5777654

experiment_id: 5781024

experiment_id: 5781872

experiment_id: 5782840

experiment_id: 5783139

experiment_id: 13702623

experiment_id: 48962799

experiment_id: 48966183

experiment_id: 49323039

experiment_id: 49369486

experiment_id: 49372349

experiment_id: 49375243

experiment_id: 49378810

experiment_id: 49381183

experiment_id: 49398168

experiment_id: 49398610

experiment_id: 49421333

experiment_id: 49439039

experiment_id: 49441740

experiment_id: 49450117

experiment_id: 49452926

experiment_id: 49453755

experiment_id: 49472150

experiment_id: 49474197

experiment_id: 49487459

experiment_id: 49491666

experiment_id: 49498922

experiment_id: 49499250

experiment_id: 49499537

experiment_id: 49501765

experiment_id: 49507799

experiment_id: 49510589

experiment_id: 49512354

experiment_id: 49518511

experiment_id: 49611047

experiment_id: 49622852

experiment_id: 49624141

experiment_id: 49643657

experiment_id: 49644084

experiment_id: 49646210

experiment_id: 49648895

experiment_id: 49658503

experiment_id: 49700925

experiment_id: 49704032

experiment_id: 49756707

experiment_id: 49769406

experiment_id: 49779648

experiment_id: 49797018

experiment_id: 49816186

experiment_id: 49822870

experiment_id: 49837689

experiment_id: 49839720

experiment_id: 49842844

experiment_id: 49898306

experiment_id: 49923468

experiment_id: 49924695

experiment_id: 49943208

experiment_id: 49944043

experiment_id: 49953431

experiment_id: 49970140

experiment_id: 49979358

experiment_id: 50022295

experiment_id: 50031689

experiment_id: 50089551

experiment_id: 50209856

}

access_level {

can_write: true

can_comment: true

can_invite: true

can_read: true

is_owner: true

}

access_state {

is_commentable: true

is_editable: true

}

}

impression_system {

version: V6_CONCURRENT_IMPRESSIONS

}

session_invariants {

app_invariants {

docs_app_load {

page_controller: SERVER

page_visibility: VISIBLE

model_source: SERVER

network_state: ONLINE

has_incremental_commands: false

has_pending_changes: false

initial_model_has_webfonts: true

app_info_load: COLD

app_info_forwarding: NONE

initial_doc_size {

sketchy_pages_count: 19

sketchy_slides_count: 7

sketchy_masters_count: 1

sketchy_layouts_count: 11

unique_image_count: 0

total_image_count: 0

}

sketchy_prerender_enabled: true

is_server_created: true

has_undeliverable_pending_changes: false

start_load_time_usec: 1674231927867000

initial_fonts_have_non_standard_weight: false

document_model_version: 1

document_feature_version: 0

initial_model_has_non_standard_weight: false

non_latin_infrastructure_v1: NON_LATIN_INFRA_V1_ENABLED

first_slide_details {

shape_count: 4

textbox_count: 2

}

first_slide_not_requested: false

editor_mode: GDOCS_MODE

offline_invariants {

extension_installed: false

hosted_app_installed: false

local_storage_offline_opted_in: false

local_storage_offline_opted_out: false

extension_manifest_version: "2"

}

compass_routing_state: NO_LOCK_OWNER

domain_font_used_in_document: false

mobile_font_woff2_state: MOBILE_FONT_WOFF2_ENABLED

group_set_for_metrics: ABSENT

converted_document: false

initial_revision: 13

preferences_at_load_docs {

name: DOCS_DISPLAY_DENSITY

value_boolean: false

}

editor_session_id: "793af75b770d7b0a"

lowest_font_metadata_schema_version: 1

shard_name: SHARD102

is_document_shared: true

document_visibility_state: PRIVATE

document_acl_count: 2

is_loaded_by_requesting_creator: true

has_summary: false

embedded_file_total_count: 0

colour_scheme: LIGHT

is_slide_library_opened_on_initial_load: false

l2_gfe_type: L2_MANAGED_PRESENTATIONS

has_parent_frame: false

resource_load_details {

resource_category: CORE_JS

resource_load_source: FROM_CACHE

}

resource_load_details {

resource_category: APP_JS

resource_load_source: FROM_CACHE

```
}
}
docs_editor {
access_mode: EDIT
is_integrated: false
client_supported_model_version: 9
document_id: "1QQI4oqwLdVx1vZYg6zaEh6_VoZCk1eN6UE84uKA67No"
}
docos {
experiment_info {
                experiment_id: 5700019
                        experiment_id: 5700036
                        experiment_id: 5700057
                        experiment_id: 5700103
                        experiment_id: 5700114
                        experiment_id: 5700133
                        experiment_id: 5700333
                        experiment_id: 5700884
                        experiment_id: 5700893
                        experiment_id: 5701034
                        experiment_id: 5701641
                        experiment_id: 5702392
                        experiment_id: 5702538
                        experiment_id: 5702785
                        experiment_id: 5703182
                        experiment_id: 5703206
                        experiment_id: 5703307
                        experiment_id: 5703575
                        experiment_id: 5703839
                        experiment_id: 5704387
                        experiment_id: 5704572
                        experiment_id: 5704621
                        experiment_id: 5704883
                        experiment_id: 5705891
                        experiment_id: 5706270
```

experiment_id: 5706523

experiment_id: 5706669

experiment_id: 5706786

experiment_id: 5706999

experiment_id: 5707047

experiment_id: 5707204

experiment_id: 5707327

experiment_id: 5707445

experiment_id: 5707609

experiment_id: 5707695

experiment_id: 5707711

experiment_id: 5707820

experiment_id: 5708235

experiment_id: 5708365

experiment_id: 5708560

experiment_id: 5708886

experiment_id: 5709085

experiment_id: 5709201

experiment_id: 5709209

experiment_id: 5709476

experiment_id: 5709673

experiment_id: 5710189

experiment_id: 5710692

experiment_id: 5711230

experiment_id: 5711550

experiment_id: 5711669

experiment_id: 5712189

experiment_id: 5712489

experiment_id: 5712556

experiment_id: 5712635

experiment_id: 5712909

experiment_id: 5712913

experiment_id: 5713195

experiment_id: 5713554

experiment_id: 5713993

experiment_id: 5714310

experiment_id: 5715322

experiment_id: 5717909

experiment_id: 5719464

experiment_id: 5719484

experiment_id: 5722141

experiment_id: 5722201

experiment_id: 5722802

experiment_id: 5723989

experiment_id: 5724217

experiment_id: 5724437

experiment_id: 5726697

experiment_id: 5727259

experiment_id: 5728004

experiment_id: 5728967

experiment_id: 5730227

experiment_id: 5730287

experiment_id: 5731837

experiment_id: 5732343

experiment_id: 5733770

experiment_id: 5734614

experiment_id: 5735136

experiment_id: 5735254

experiment_id: 5735808

experiment_id: 5736413

experiment_id: 5737256

experiment_id: 5737802

experiment_id: 5739780

experiment_id: 5740188

experiment_id: 5740343

experiment_id: 5740816

experiment_id: 5741976

experiment_id: 5742726

experiment_id: 5743146

experiment_id: 5743789

experiment_id: 5744290

experiment_id: 5744350

experiment_id: 5745460

experiment_id: 5746726

experiment_id: 5746786

experiment_id: 5747218

experiment_id: 5747943

experiment_id: 5749257

experiment_id: 5750112

experiment_id: 5750878

experiment_id: 5750956

experiment_id: 5751159

experiment_id: 5752152

experiment_id: 5752676

experiment_id: 5753663

experiment_id: 5753683

experiment_id: 5754311

experiment_id: 5754830

experiment_id: 5755411

experiment_id: 5756697

experiment_id: 5757324

experiment_id: 5758499

experiment_id: 5758638

experiment_id: 5758676

experiment_id: 5759280

experiment_id: 5759564

experiment_id: 5760169

experiment_id: 5760329

experiment_id: 5760452

experiment_id: 5760472

experiment_id: 5762731

experiment_id: 5763275

experiment_id: 5763519

experiment_id: 5764067

experiment_id: 5764468

experiment_id: 5768934

experiment_id: 5770337

experiment_id: 5771105

experiment_id: 5777654

experiment_id: 5781024

experiment_id: 5781872

experiment_id: 5782840

experiment_id: 5783139

experiment_id: 13702623

experiment_id: 48962799

experiment_id: 48966183

experiment_id: 49323039

experiment_id: 49369486

experiment_id: 49372349

experiment_id: 49375243

experiment_id: 49378810

experiment_id: 49381183

experiment_id: 49398168

experiment_id: 49398610

experiment_id: 49421333

experiment_id: 49439039

experiment_id: 49441740

experiment_id: 49450117

experiment_id: 49452926

experiment_id: 49453755

experiment_id: 49472150

experiment_id: 49474197

experiment_id: 49487459

experiment_id: 49491666

experiment_id: 49498922

experiment_id: 49499250

experiment_id: 49499537

experiment_id: 49501765

experiment_id: 49507799

experiment_id: 49510589

experiment_id: 49512354

experiment_id: 49518511

experiment_id: 49611047

experiment_id: 49622852

experiment_id: 49624141

experiment_id: 49643657

experiment_id: 49644084

experiment_id: 49646210

experiment_id: 49648895

experiment_id: 49658503

experiment_id: 49700925

experiment_id: 49704032

experiment_id: 49756707

experiment_id: 49769406

experiment_id: 49779648

experiment_id: 49797018

experiment_id: 49816186

experiment_id: 49822870

experiment_id: 49837689

experiment_id: 49839720

experiment_id: 49842844

experiment_id: 49898306

experiment_id: 49923468

experiment_id: 49924695

experiment_id: 49943208

experiment_id: 49944043

experiment_id: 49953431

experiment_id: 49970140

experiment_id: 49979358

experiment_id: 50022295

experiment_id: 50031689

experiment_id: 50089551

experiment_id: 50209856

}

app_load_counts {

```
 comments: 0
 suggestions: 0
 assignments: 0
 }
 app_load_anchored_counts {
 comments: 0
 suggestions: 0
 assignments: 0
 }
 notification_level: ALL
 edit_notification_level: false
 }
}
build_info {
 rapid_candidate_label: "editors.presentations-frontend_20230110.02_p3"
}
os {
 os_type: OS_X
 os_version: "10.15"
}
job set: PROD
user_channel: RELEASE
navigation_timing {
 navigation_start_usec: 1674231927268000
 redirect_start_usec: 1674231927268000
 redirect_end_usec: 1674231927268000
 fetch_start_usec: 1674231927268000
 domain_lookup_start_usec: 1674231927268000
 domain_lookup_end_usec: 1674231927268000
 connect_start_usec: 1674231927268000
 connect_end_usec: 1674231927268000
 request_start_usec: 1674231927289000
 response_start_usec: 1674231927795000
 response_end_usec: 1674231927795000
 redirect_count: 0
```

navigation_type: NAVIGATE
}
device {
num_google_accounts: 1
hardware_concurrency: 6
}
document_open_source {
source {
url_source {
usp: "drive_web"
is_workspaceized: false
is_projector_redirection_on_failure_enabled: false
has_chrome_os_url_hint: false
}
}
}
browser {
is_browser_supported: true
is_firefox_electrolysis: true
is_touch_supported: false
are_pointer_events_supported: true
is_likely_spoofed_edge: false
}
display_invariants {
display_extended_status: DISPLAY_EXTENDED_STATUS_API_NOT_AVAILABLE
display_count_status: DISPLAY_COUNT_STATUS_API_NOT_AVAILABLE
} } }", "http_lang": "en-US,en;q=0.5"}"

Google improvements audit logs

Google has made the following commitment on audit logs:

"In response to our commitment to expand the availability of admin audit logs, Google identified and will launch new audit logs (and update some existing audit logs) ***across 19 Workspace Core Services*** *(including EDU) by the end of 2022. The following table describes those new (and updated) events triggering audit logs."*

This report excludes the Google Voice service.

Assignments [out of scope of this verification report]

1. Course created
2. Course deleted
3. User joined course
4. User removed from course
5. Course work published
6. Submission state changed

Calendar

1. Transfer event
2. Export Calendar (web)
3. Create / update / delete appointment schedule
4. Create / update / delete recurring event, as recurring
5. Print Calendar (web)
6. Print event (web)

Chat in Gmail

1. Room details updated
2. Room name updated
3. Message deleted
4. User left room
5. Reaction added
6. Reaction removed
7. User blocked
8. User unblocked
9. Room blocked
10. Room unblocked
11. History turned on
12. History turned o_
13. Unread timestamp updated
14. Custom status updated

Chrome Sync [out of scope of this verification report]

1. User changed encryption settings
2. User selected to clear data from https://chrome.google.com/sync
3. User came online with a new Chrome client
4. User opted in to Chrome sync
5. APP - (add/delete)

6. Autofill information (add/delete)

7. Credit card details (add/delete)

8. Bookmark (add/delete)

9. Chrome extension (add/delete)

10. Password (add/delete)

11. Reading list (add/delete)

12. Web app (add/delete)

13. Authorisation server for printers (add/delete)

14. Wallet metadata (add/delete)

15. Web Auth credentials (add/delete)

16. User requested to export data from Google Takeout

17. User reused their Google password

18. User used their Google password

Classroom

1. [Updated existing event] User joined course (includes previous course role info now, i.e. whether they were a student)

2. User invited to own course

3. New user owns course

4. Transferred ownership of course

5. Updated announcement

6. Set draft grade

7. Unset draft grade

8. Set grade

9. Unset grade

10. Created add-on attachment

11. Deleted add-on attachment

12. Updated add-on attachment

13. Updated add-on-attachment submission grade

14. Grade export for course work

15. Originality report created

16. Guardian summaries settings updated for course

17. Guardian invited for student

18. Guardian responded to invite

19. Guardian removed for student

20. Guardian updated email

21. [Updated existing event] Published course work (includes attachment types now)

22. [Updated existing event] Published announcement (includes attachment types now)

23. Grade export for submission

24. Default guardian summaries settings updated for teacher

25. Updated course work

Cloud search [out of scope of this verification report]

1. Search

2. Suggest

3. ListQuerySources

Contacts

1. Create a label

2. Rename a label

3. Delete a label

4. Create singular new contact

5. Create bulk new contacts

6. Delete a contact

7. Edit a contact

8. Merge contacts manually

9. Add to contacts

10. Print

11. Import

12. Export

13. Hide (Archive) a contact

14. Accept a merge and fix suggestion

15. Grant user delegate access

16. Remove user's delegate access

17. Revert contact list to previous date

18. Recover trashed contact

19. Permanently delete trashed contact

20. Undo a mutate action

Docs [part of DRIVE logs, with Sheets and Slides]

1. Email collaborators

2. Report abuse/copyright

3. Add Comment

4. Accept/Reject suggestions

Drive

1. Adding new caption from Drive
2. Downloading captions
3. Deleting the captions
4. Keep Forever option
5. Deleting an old version
6. Report abuse for google file
7. Request access for file and owner receives email
8. Email collaborators

Gmail

1. Blocked sender
2. Draft saved
3. Permanently deleted an email

Groups [out of scope of this verification report]

1. Change email subscription type
2. Join groups via mail command
3. Leave groups via mail command

Jamboard [out of scope of this verification report]

1. Request for edit access
2. Verify that user is able to Share Jam as PDF
3. Verify that user is able to Share this frame as an image

Meet

1. Accept/Decline a Knocking request
2. Invite a user via email
3. Ringing/Calling another Meet user
4. Dial out to a PSTN user
5. Present a tab/window/screen
6. Start/stop a recording
7. Start/stop a live streaming (private/public)
8. Create a question
9. Answer a question
10. Create a poll
11. Respond a poll
12. Create/Stop call transcript
13. Attach a whiteboarding

Profile data [out of scope of this verification report]

1. Update / Delete of the following profile fields (if available):

2. Name

3. Birthday

4. About

5. Email

6. Phone

7. Gender

8. Website

9. Address

10. Location

11. Photo

12. Portrait Photo

13. Organisation

14. Nickname

15. IM (instant message)

16. Pronoun

17. Language

18. File As

19. Relation

20. External ID

21. Posix Account

22. Ssh Public Key

Sheets

1. Commentators comment insertion

2. Stop scheduled script

Sites [out of scope of this verification report]

1. Log an event when the user selects "Publish" on the 'Publish your site' modal.

2. Replace the url string before /p/ and the site will export

Slides [section DRIVE logs]

1. Email collaborators

Tasks

1. Task Creation

2. Task Completion

3. Task Uncompletion

4. Task Deletion

5. Task Undeletion

6. Task Assigned

7. Task Unassigned

8. Task Reassigned

9. Task title change

10. Task due date/time change

11. Task Modified (covers description change, starred, unstarred)

12. Task moved between task lists

13. Task list creation

14. Task list deletion

15. All completed tasks on a list deleted

16. Task list title change

17. Task list structure change

18. Recurring task created

19. Recurring schedule added to a task

20. Title changed for a recurring task

21. Recurring task modified

22. Recurring schedule deleted

Examples of new Workspace for Education audit logs

Figure 45: User log events

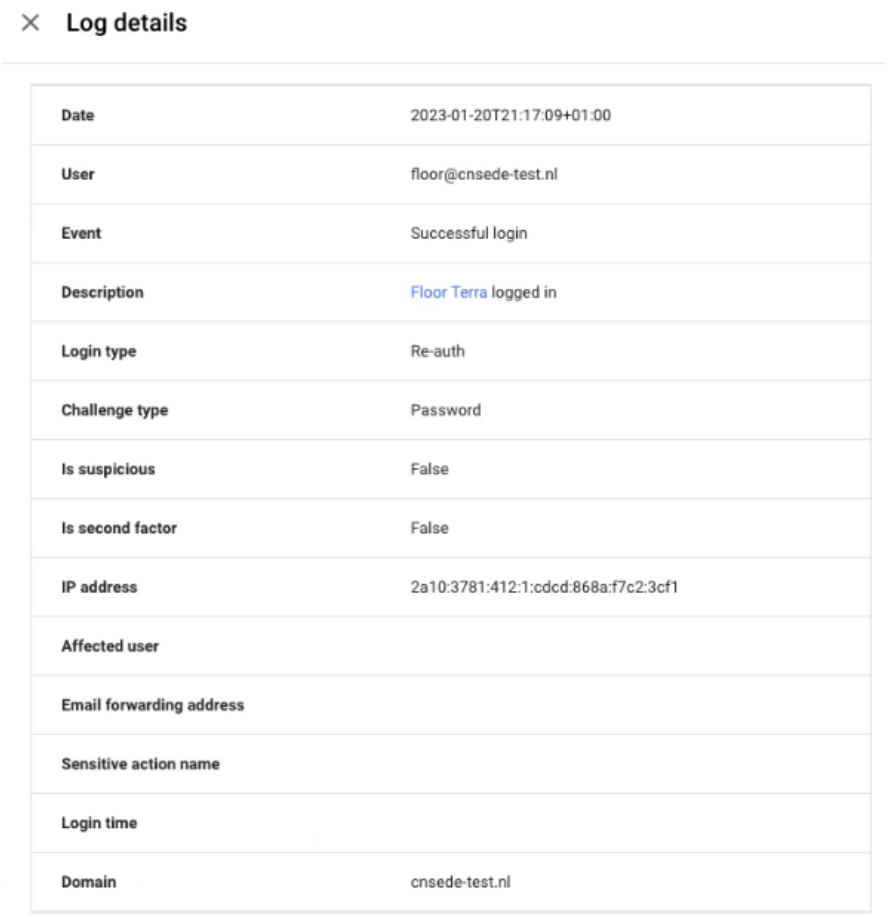
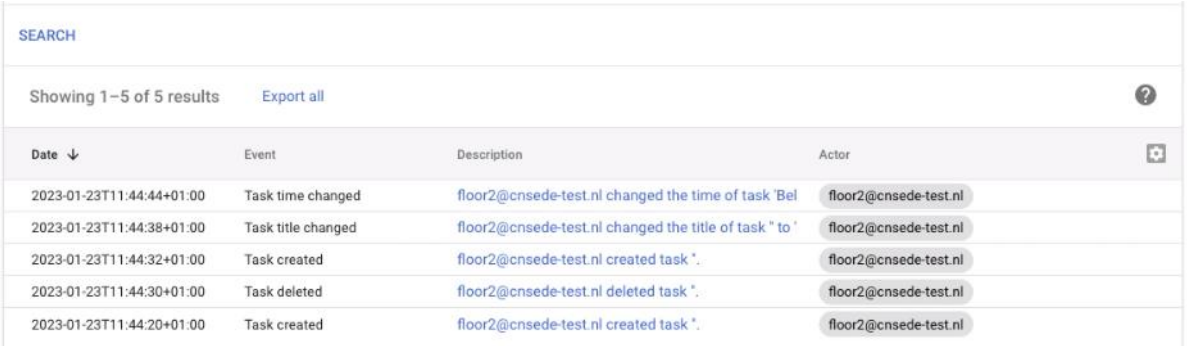


Figure 46: Two screenshots of Task log events: overview actions and details of 1 action



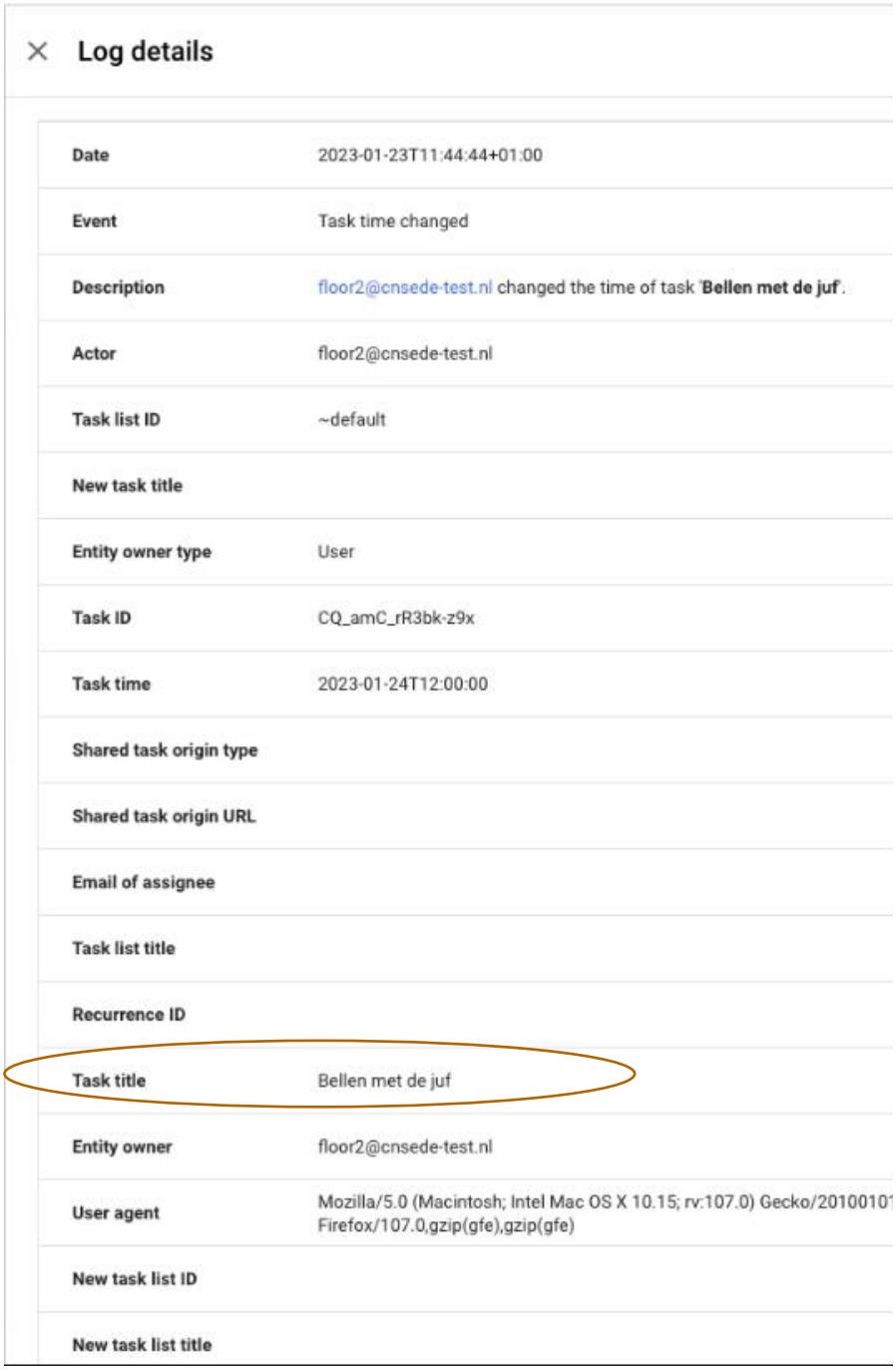
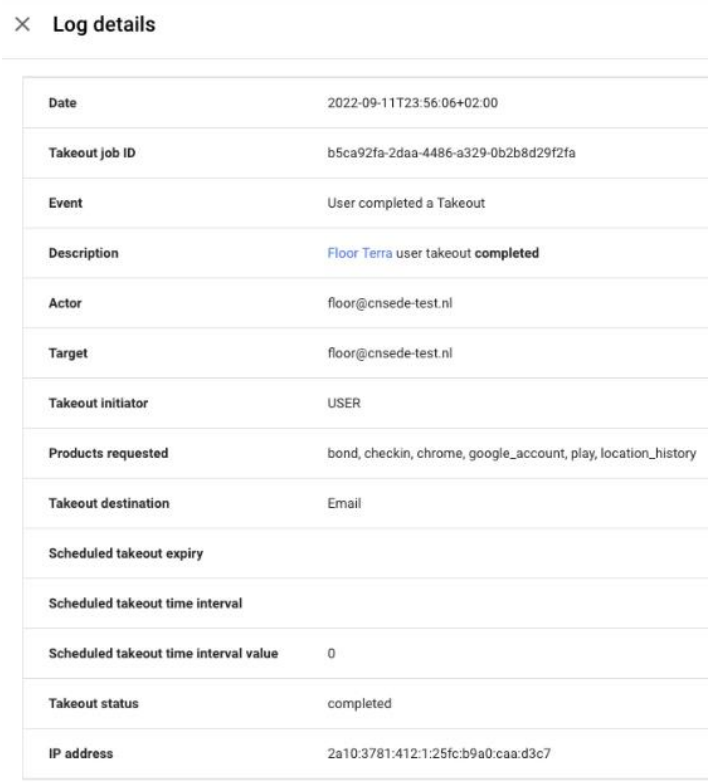

Log details
Date
2023-01-23T11:44:44+01:00
Event
Task time changed
Description
floor2@cnsede-test.nl changed the time of task 'Bellen met de juf'.
Actor
floor2@cnsede-test.nl
Task list ID
~default
New task title
Entity owner type
User
Task ID
CQ_amC_rR3bk-z9x
Task time
2023-01-24T12:00:00
Shared task origin type
Shared task origin URL
Email of assignee
Task list title
Recurrence ID
Task title
Bellen met de juf
Entity owner
floor2@cnsede-test.nl
User agent
Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:107.0) Gecko/2010010
Firefox/107.0,gzip(gfe),gzip(gfe)
New task list ID
New task list title

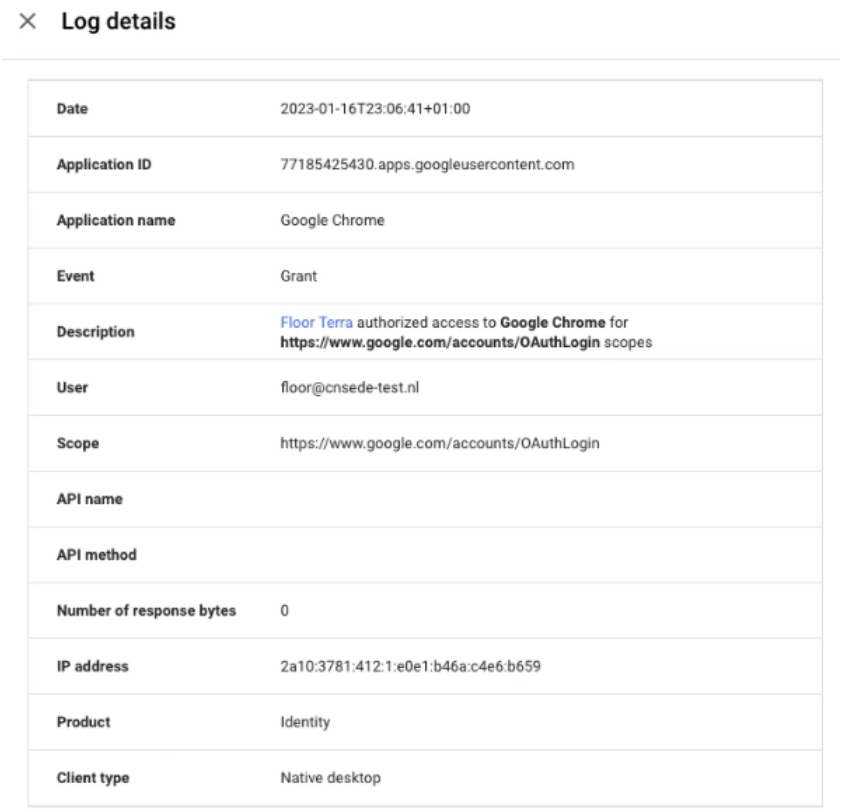
Figure 47: Screenshot of Takeout log



Log details

Date	2022-09-11T23:56:06+02:00
Takeout job ID	b5ca92fa-2daa-4486-a329-0b2b8d29f2fa
Event	User completed a Takeout
Description	Floor Terra user takeout **completed**
Actor	floor@cnsede-test.nl
Target	floor@cnsede-test.nl
Takeout initiator	USER
Products requested	bond, checkin, chrome, google_account, play, location_history
Takeout destination	Email
Scheduled takeout expiry	
Scheduled takeout time interval	
Scheduled takeout time interval value	0
Takeout status	completed
IP address	2a10:3781:412:1:25fc:b9a0:caa:d3c7

Figure 48: Screenshot of Oauth approval login on Chrome



Log details

Date	2023-01-16T23:06:41+01:00
Application ID	77185425430.apps.googleusercontent.com
Application name	Google Chrome
Event	Grant
Description	Floor Terra authorized access to **Google Chrome** for **https://www.google.com/accounts/OAuthLogin** scopes
User	floor@cnsede-test.nl
Scope	https://www.google.com/accounts/OAuthLogin
API name	
API method	
Number of response bytes	0
IP address	2a10:3781:412:1:e0e1:b46a:c4e6:b659
Product	Identity
Client type	Native desktop

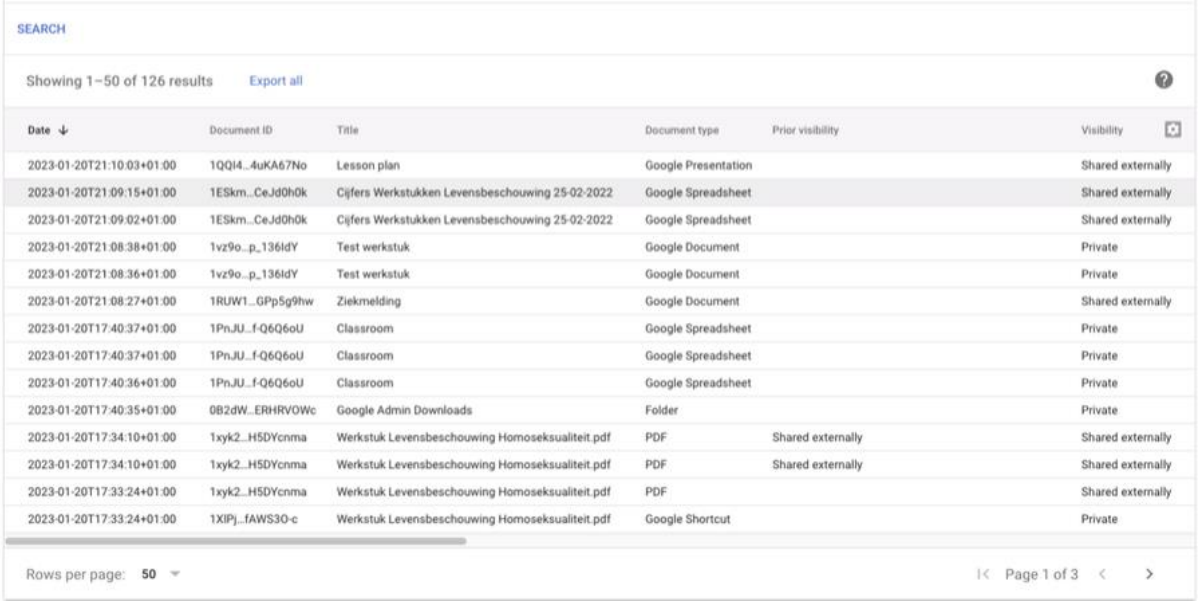
Figure 49: Two screenshots of (long) Google Meet log

Log details

Date	2023-01-20T21:11:01+01:00
Meeting code	ITOSUADZCU
Conference ID	WlmUh_DbDzQJq0dQVRI1DxIMOAIoABgCEAgligk
Event	Endpoint left
Description	The endpoint left a video meeting
Actor	floor@cnsede-test.nl
Actor name	Floor Terra
Actor identifier type	Email address
Calendar event ID	
Organiser email	floor@cnsede-test.nl
Participant outside organisation	False
Client type	iOS
Product type	Google Meet
Duration (seconds)	25
Endpoint ID	hub_ios_5mNuH379ZCA
IP address	2a10:3781:412:1:5090:43d4:970:9b00
Country	NL
City	Amersfoort
Call rating out of 5	0

Call rating out of 5	0
Network statistics	
Audio statistics	
Video send statistics	Duration (sec): 24, Bitrate Kbps Mean: 205, Packet Loss M Packet Loss Mean: 0, Long Side Median: 320, Short Side M 180, FPS Mean: 29
Video receive statistics	
Presentation send statistics	
Presentation receive statistics	
Livestream view page ID	
Action reason	
Action description	
Target display names	
Target	
Target phone number	
Broadcast state	
Streaming session state	
Target user count	0
Action time	

Figure 50: Screenshot of the (first few columns of) Drive log events



SEARCH

Showing 1–50 of 126 results Export all

Date	Document ID	Title	Document type	Prior visibility	Visibility
2023-01-20T21:10:03+01:00	1QQI4...4uKA67No	Lesson plan	Google Presentation		Shared externally
2023-01-20T21:09:15+01:00	1ESkm...CeJd0h0k	Cijfers Werkstukken Levensbeschouwing 25-02-2022	Google Spreadsheet		Shared externally
2023-01-20T21:09:02+01:00	1ESkm...CeJd0h0k	Cijfers Werkstukken Levensbeschouwing 25-02-2022	Google Spreadsheet		Shared externally
2023-01-20T21:08:38+01:00	1vz9o...p_136IdY	Test werkstuk	Google Document		Private
2023-01-20T21:08:36+01:00	1vz9o...p_136IdY	Test werkstuk	Google Document		Private
2023-01-20T21:08:27+01:00	1RUW1...GPp5g9hw	Ziekmelding	Google Document		Shared externally
2023-01-20T17:40:37+01:00	1PnJU...f-Q6Q6oU	Classroom	Google Spreadsheet		Private
2023-01-20T17:40:37+01:00	1PnJU...f-Q6Q6oU	Classroom	Google Spreadsheet		Private
2023-01-20T17:40:36+01:00	1PnJU...f-Q6Q6oU	Classroom	Google Spreadsheet		Private
2023-01-20T17:40:35+01:00	0B2dW...ERHRVOWc	Google Admin Downloads	Folder		Private
2023-01-20T17:34:10+01:00	1xyk2...H5DYcnma	Werkstuk Levensbeschouwing Homoseksualiteit.pdf	PDF	Shared externally	Shared externally
2023-01-20T17:34:10+01:00	1xyk2...H5DYcnma	Werkstuk Levensbeschouwing Homoseksualiteit.pdf	PDF	Shared externally	Shared externally
2023-01-20T17:33:24+01:00	1xyk2...H5DYcnma	Werkstuk Levensbeschouwing Homoseksualiteit.pdf	PDF		Shared externally
2023-01-20T17:33:24+01:00	1XIPj...fAWS3O-c	Werkstuk Levensbeschouwing Homoseksualiteit.pdf	Google Shortcut		Private

Rows per page: 50 Page 1 of 3

Table 5: Overview contents of Drive log: 39 types of events

Title	Document type	Prior visibility

Visibility	Event	Description
Actor	Owner	Target
IP address	Old value	New value
Recipient doc.	Domain	Label title
Label field display name	Old value IDs	New value IDs
Audience	Old publish visibility value	New publish visibility value
Billable	Visitor	Copy type
Requested access role	Video caption name	Revision ID
Revision create timestamp	Execution ID	Data connection ID
Execution trigger	Delegating principal	Query type
Script trigger source app	Script trigger type	Script container app
Script container ID	Script trigger ID	Recipients

Figure 51: Contact details log

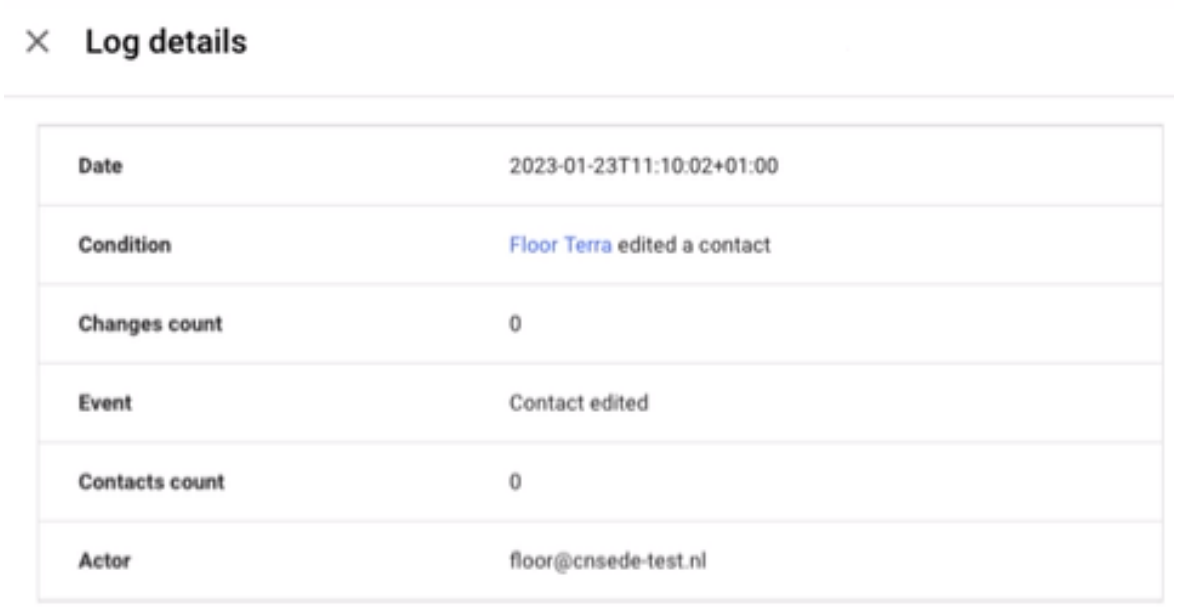
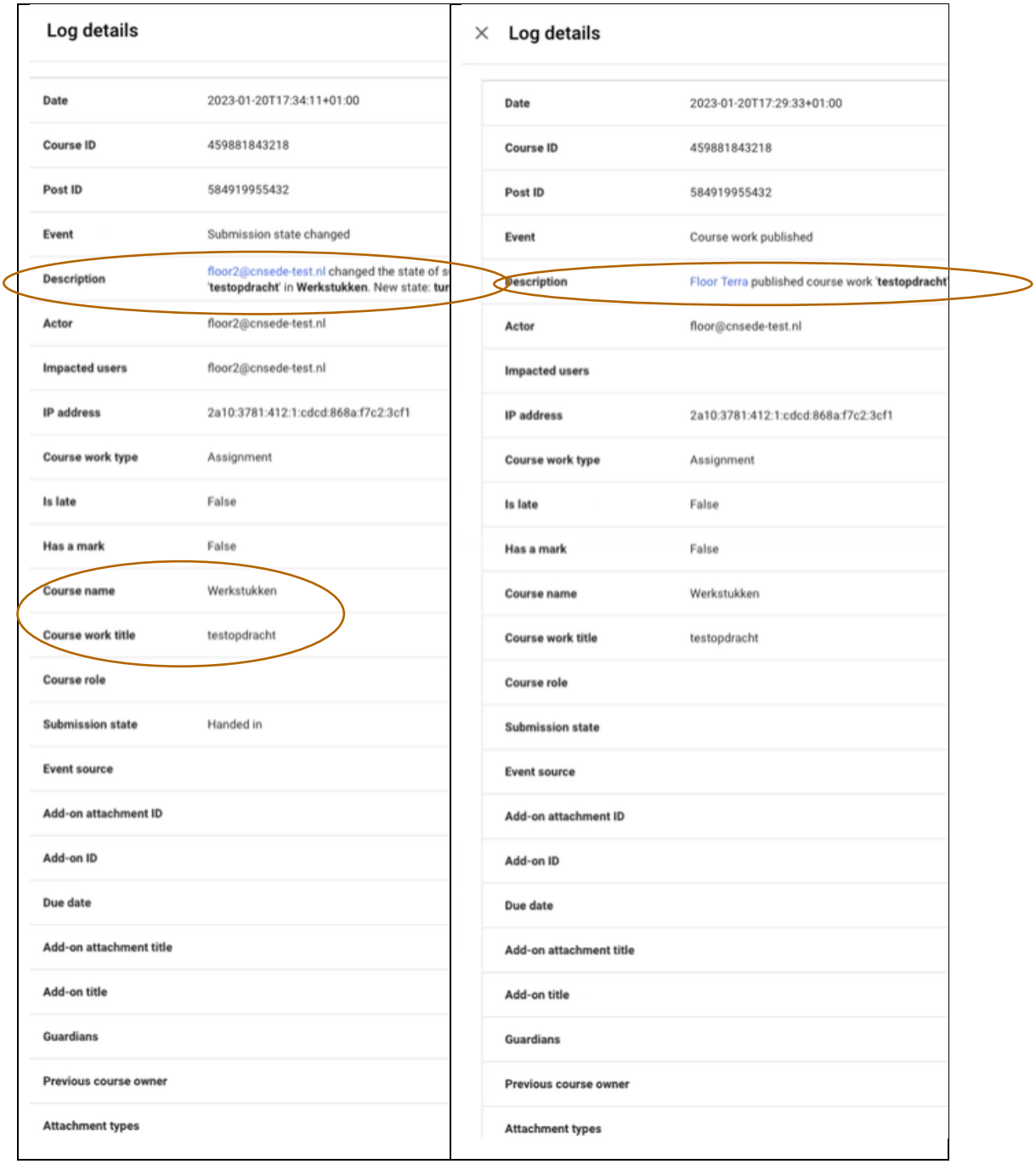


Figure 52: Screenshots of Classroom logs, both of teacher and student



Log details

Date	2023-01-20T17:34:11+01:00
Course ID	459881843218
Post ID	584919955432
Event	Submission state changed
Description	floor2@cnsede-test.nl changed the state of s 'testopdracht' in Werkstukken. New state: tur
Actor	floor2@cnsede-test.nl
Impacted users	floor2@cnsede-test.nl
IP address	2a10:3781:412:1:cdcd:868a:f7c2:3cf1
Course work type	Assignment
Is late	False
Has a mark	False
Course name	Werkstukken
Course work title	testopdracht
Course role	
Submission state	Handed in
Event source	
Add-on attachment ID	
Add-on ID	
Due date	
Add-on attachment title	
Add-on title	
Guardians	
Previous course owner	
Attachment types	

Log details

Date	2023-01-20T17:29:33+01:00
Course ID	459881843218
Post ID	584919955432
Event	Course work published
Description	Floor Terra published course work 'testopdracht'
Actor	floor@cnsede-test.nl
Impacted users	
IP address	2a10:3781:412:1:cdcd:868a:f7c2:3cf1
Course work type	Assignment
Is late	False
Has a mark	False
Course name	Werkstukken
Course work title	testopdracht
Course role	
Submission state	
Event source	
Add-on attachment ID	
Add-on ID	
Due date	
Add-on attachment title	
Add-on title	
Guardians	
Previous course owner	
Attachment types	

Figure 53: Screenshot admin log events

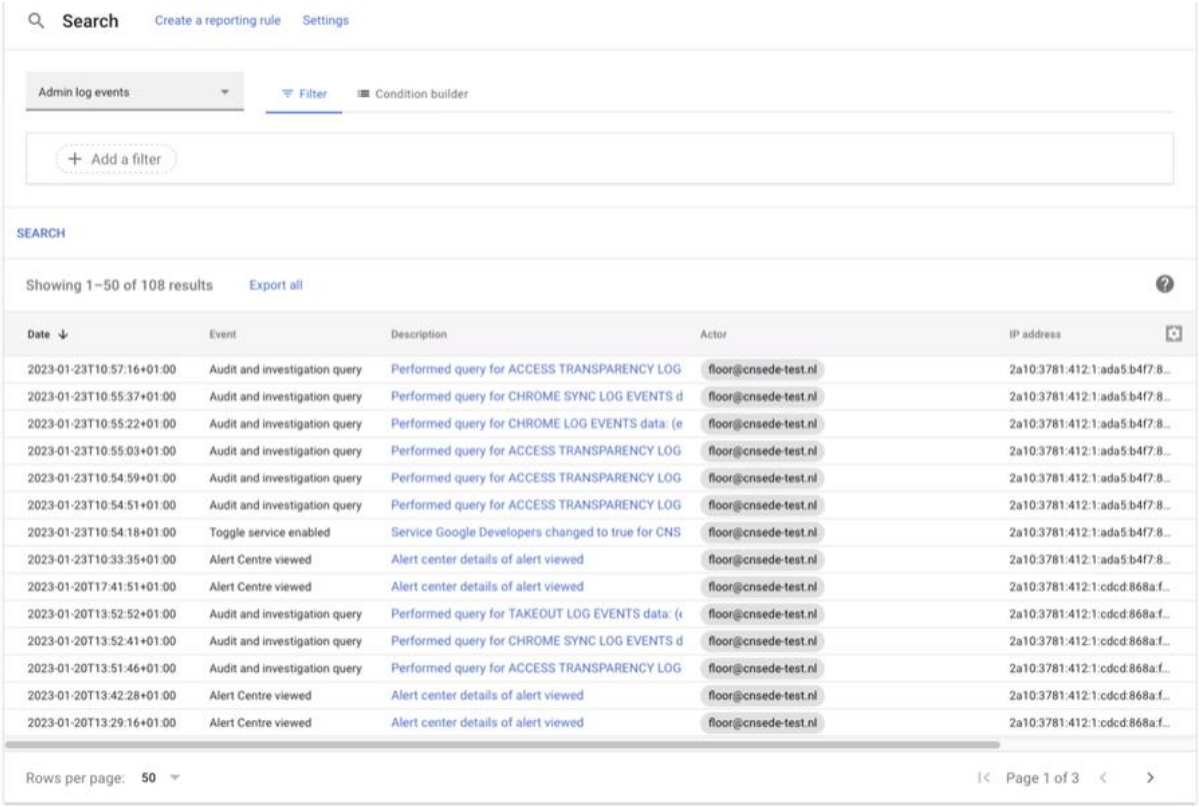


Figure 54: Screenshot Calendar log events (change command)

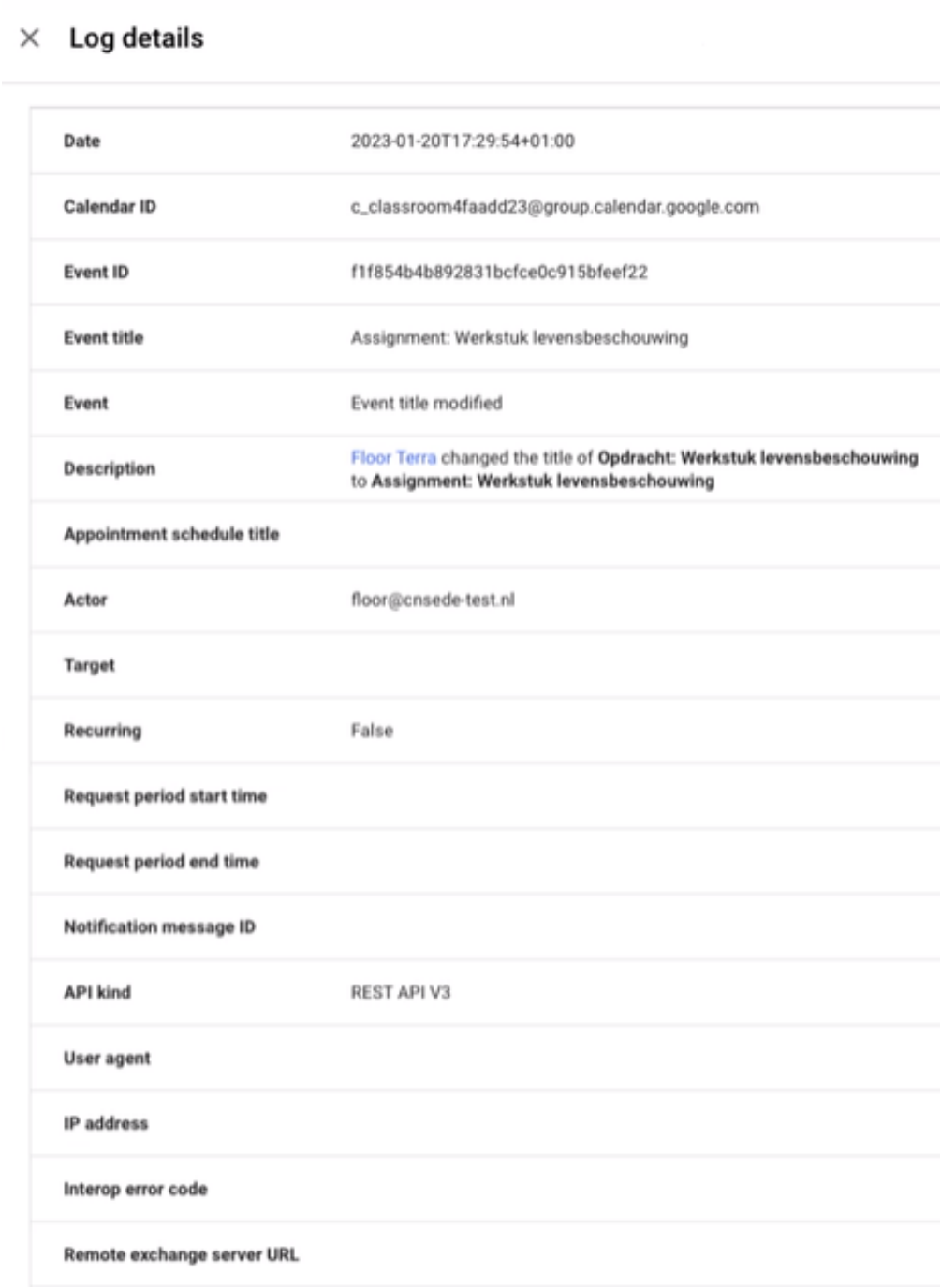


Figure 55: Screenshots of Chrome Sync log events, overview and details,