New findings verification review Google Workspace Enterprise

15 May 2024

Sjoera Nas and Floor Terra

Introduction

At the request of the Dutch government strategic vendor manager for Microsoft, Google Cloud and Amazon Web Services (hereinafter SLM Rijk), Privacy Company has verified whether Google had mitigated the 9 high risks for data subjects when using the paid versions of Google Workspace Enterprise as those risks are described in the June 2021 update DPIA.[1] The verification report concludes the 9 high risks are mitigated, or reduced to a low risk.

However, the verification report also mentions that the researchers saw five new processing operations that could potentially lead to high risks. These extra findings were discussed with Google, and all five of these risks have also been mitigated.

Below, the new findings are explained in five separate paragraphs.

Summary table of findings and (mitigated) risks

The table shows the five extra findings and the risks they could potentially cause for government employees, including admins, using Google Workspace Enterprise. The third column shows the mitigating measures taken by Google, while the fourth column shows the measures advised to government organisations. If the measure mitigates the risk, the box is accordingly coloured green.

Table 1: (potentially) high risks, findings, measures taken by Google and recommended measures for government organisations

Original risk(s)	Finding	Measure taken by Google	Measure recommended to government organisations
Lack of purpose limitation Customer Data and Diagnostic Data	Google can show surveys to end users in the Core Services.	none	Warn users not to participate in surveys
Lack of purpose limitation Customer Data No legal ground for Google and schools/universities No privacy by default	Introduction of *Smart Features* such as Smart Compose that use machine learning. Role of Google not clear/not documented. Users are nudged to enable the services.	*Smart features* are turned off by default for domains based in Europe, but users can still enable. Google has committed to process all Content and Diagnostic Data from Smart Features within the processor role (apart from the limited agreed legitimate business	

[1] 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.

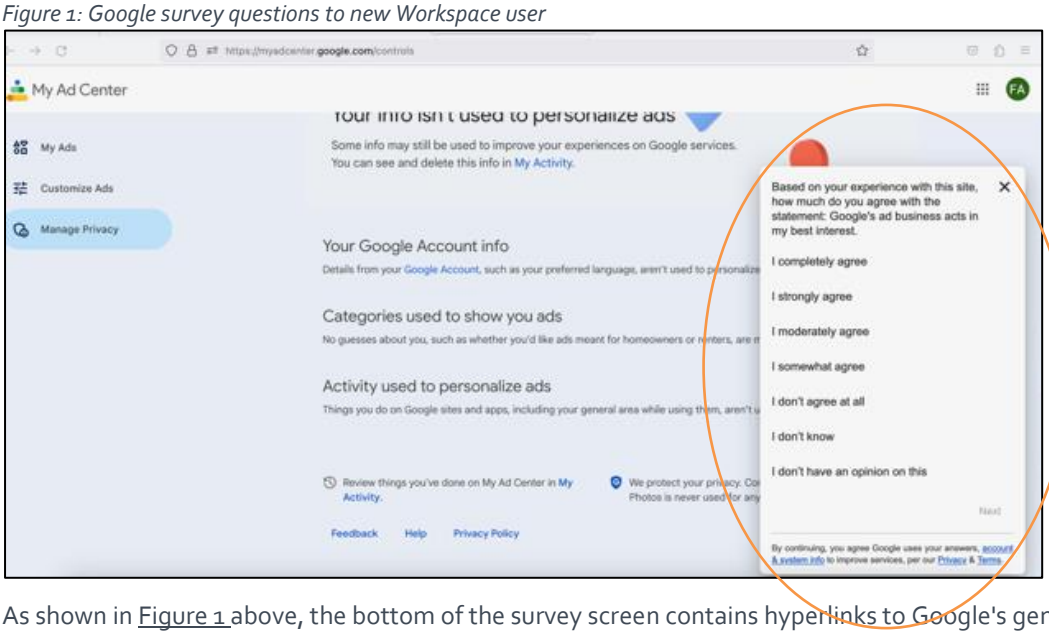
		purposes) and results stay in customer domain.	
No legal ground for Google and schools/universities Missing privacy controls	Use of the multi-purpose NID-cookie when logging in to a Workspace account and when looking up the Google Cloud Privacy Notice.	Google has informed SLM that it does not use the NID-cookie set in the Workspace environment or when looking up the Google Cloud Privacy Notice for advertising purposes. When signed-out, users must provide consent for the use of the NID-cookie and other non-essential cookies for advertising on Google websites and on third party websites with Google advertising.	-
		Google improved the text of the cookie banner on the GCPN page to commit that the GCPN site does not use cookies for advertising.	
Lack of transparency	Google collects Content Data from spelling check in telemetry events and directly identifiable personal data (name/email address). The retention period of these events is unknown.	Google has explained, and published an explanation on 9 June 2023 why it is necessary to collect these data, and explained that the retention period is 30 days.	-
No legal ground for Google and schools/universities	New guidance from the EDPB about high risks of CSAM scanning.	Google has confirmed that it only scans for **known** CSAM, no use of machine learning/AI.	-

Finding 1: Google asks survey questions in customer environment

Immediately after creating a new Google Workspace account and viewing the default setting for personalised ads in Google's My Ad Center, a new user was presented with a series of survey questions from Google, about Google's ad business. In total, Google showed seven screens with questions about the use of data for personalised ads. See Figure 1 below.

Even though Privacy Company only observed this survey in a different test environment (in Workspace for Education) and did not retest in a Workspace Enterprise environment, there is no reason to believe that Google did not ask these questions in the Enterprise environment, since Google explained that the survey was shown in 'My Ad Center', which is not part of the Core Workspace services.

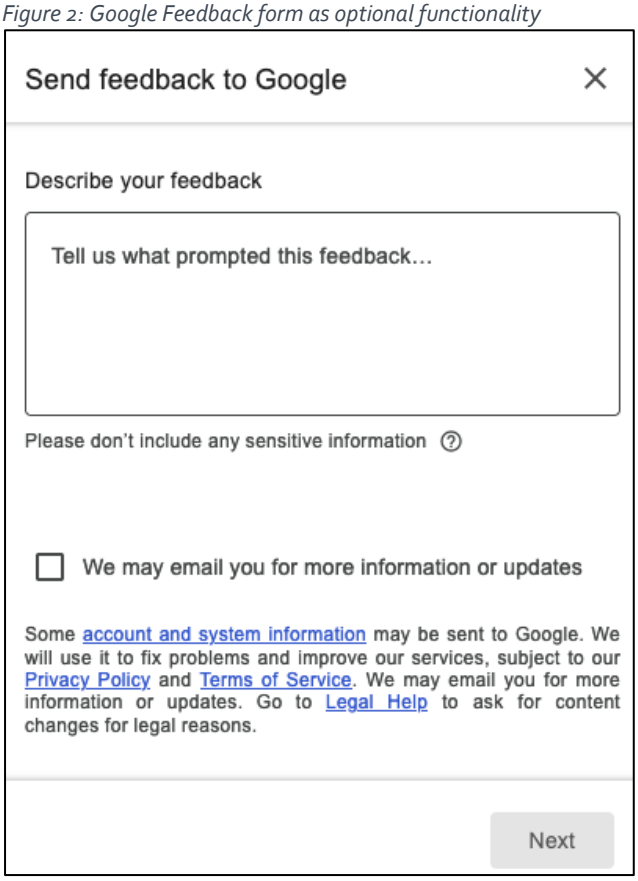
Figure 1: Google survey questions to new Workspace user



As shown in Figure 1 above, the bottom of the survey screen contains hyperlinks to Google's general privacy statement and terms and conditions. A privacy expert can infer from these references that Google permits itself to process the data for its own commercial purposes, acting as an independent data controller. For ordinary end users, this is not clear. Moreover, Google's questions are suggestive about the usefulness of personalised ads (with many more agree and don't know answers than disagree options). It appeared Google collected these answers to substantiate a legitimate interest as a legal basis for the processing of personal data for behavioural advertising. At the time, the EDPB ruled in sanction proceedings against Facebook/Meta that the legal basis of contract (Article 6(1)(b) of the GDPR) could not be used for this purpose.[2] On 27 October 2023, the EDPB also ruled out the use of necessity for a legitimate business interest as legal basis for behavioural advertising.

[2] EDPB decision on the Irish DPC's draft decision on Facebook, URL: https://edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-32022-dispute-submitted_en EDPB press release of 12 January 2023 at https://edpb.europa.eu/news/news/2023/facebook-and-instagram-decisions-important-impact-use-personal-data-behavioural_en . Press release EDPB, Urgent Binding Decision on processing of personal data for behavioural advertising by Meta, 27 October 2023, URL: https://edpb.europa.eu/news/news/2023/edpb-urgent-binding-decision-processing-personal-data-behavioural-advertising-meta_en.

Figure 2: Google Feedback form as optional functionality



In reply to this finding, Google explained that it can present surveys in the Core Services, aimed at understanding how satisfied Workspace users are with the functionality of the specific Core service they are using, as part of the contractually agreed Legitimate Business Purposes. Google also explained that the questions about behavioural advertising were not commercial, as Google will not show commercial surveys in the Core Services. Google did confirm it can show other types of surveys in the core Workspace Enterprise services.

However, the agreed purpose was specifically limited to the use of a Feedback Form shown in that end users can optionally use to tell Google about their experience. As a mitigating measure, government organisations should tell their employees not to use this feature (not answer any Google surveys), as it results in disclosure of personal data to Google as a third party, outside of its processor role.

Conclusion: high risk can be mitigated by government organisations
Government organisations must warn employees not to participate in surveys.

Finding 2: Unclear role of Google in new Smart Features

During the verification process, Privacy Company noticed that Google had introduced a new service, **Smart Compose**. That service uses machine learning, Google explains: "*Use Smart Compose in Google Documents and Presentations to write documents faster and easier. Smart Compose is also available for responses in Spreadsheets and Drawings. This feature uses machine learning to give suggestions as you type.*"[3] Google also explains that administrators can centrally disable this new service.

[3] Google, Workspace administrator help, Turn Smart Compose on or off for users, URL: https://support.google.com/a/answer/10020933?hl=nl .

Figure 3: Google explanation for turning off Smart Compose

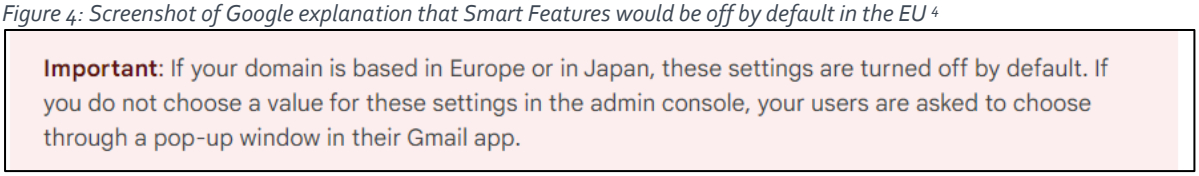
Smart Compose uitzetten

Smart Compose staat standaard aan voor gebruikers van Google Documenten, Presentaties, Spreadsheets en Tekeningen. Zo zet u de functie uit:

1. Log in bij de Google Beheerdersconsole.
   Log in met uw *beheerdersaccount* (dit eindigt *niet* op @gmail.com).
2. Ga in de Beheerdersconsole naar Menu > **Apps** > **Google Workspace** > **Drive en Documenten** > **Functies en apps**.
3. Selecteer in het gedeelte Smart Compose de optie **Niet toestaan dat gebruikers Smart Compose-suggesties zien**.

Even if government administrators do no enable Smart Compose for Gmail, it is still available to users because Google provides this functionality by default. Users are presented with a choice screen asking them to continue using the service (*Continue with Smart Features*). This is not entirely clear from Google's public explanation. Google's explanation in Figure 5 below suggests the opposite, that Smart Features would actually be off by default in the EU, and that the user has to make an effort to activate the services.

Figure 4: Screenshot of Google explanation that Smart Features would be off by default in the EU [4]

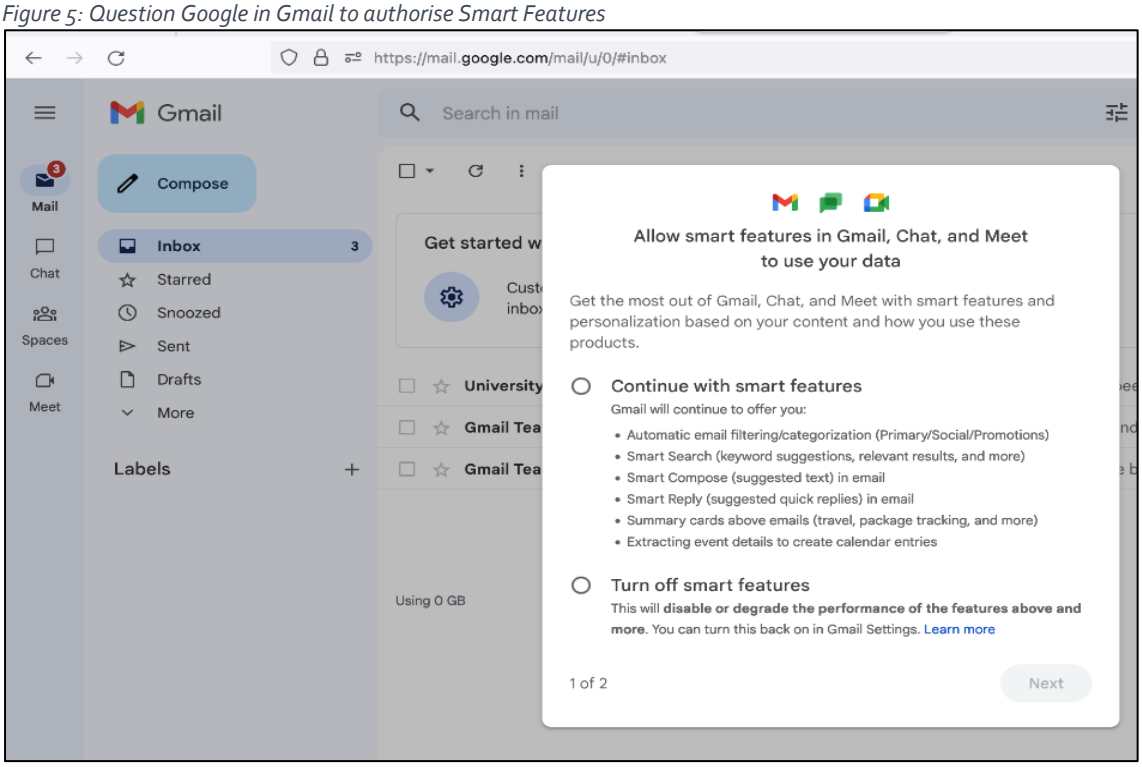


Important: If your domain is based in Europe or in Japan, these settings are turned off by default. If you do not choose a value for these settings in the admin console, your users are asked to choose through a pop-up window in their Gmail app.

Google gives users a choice in Gmail to continue with Smart Features, or to turn them off. For the 'off' option, Google gave a warning that turning the service off would result in the features and 'more' being disabled or degraded.

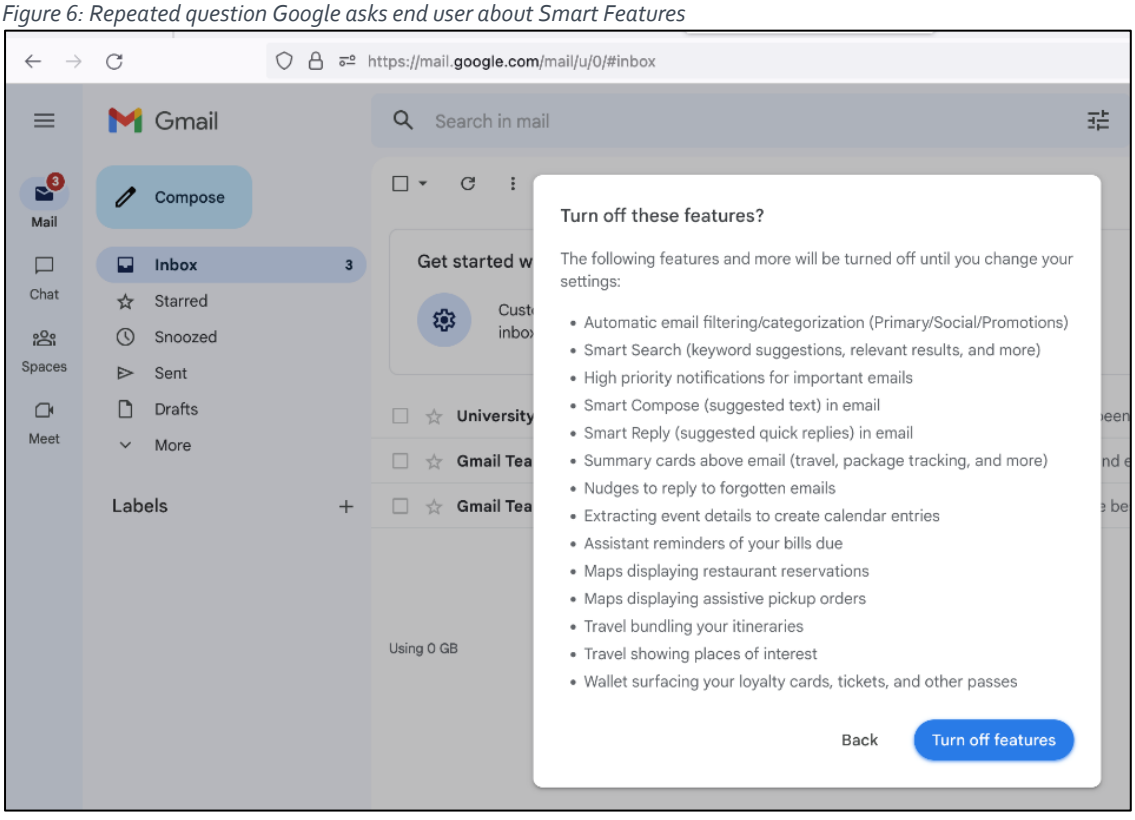
[4] Google, Turn on or off Gmail, Chat and Meet smart features and personalization (Region specific), URL: https://support.google.com/a/answer/10095404?hl=en . See also Smart features & controls in Google products, URL: https://support.google.com/mail/answer/10079371?hl=en .

Figure 5: Question Google in Gmail to authorise Smart Features



When the test user clicked (anyway) on the bottom option 'Turn off smart features', Google displayed a new question asking if the user really wanted to turn off the service. See Figure 7 below.

Figure 6: Repeated question Google asks end user about Smart Features



Due to the unclear wording of the negative consequences of turning off, Google is steering towards consent (what does degradation of 'more' mean?). This is a form of pushing (nudging) on consent.

Initially, it was not clear whether the data processing of these Smart Features was covered by the data processing agreement, and whether help with 'writing' is also a kind of spelling and grammar checker.

Google has since published that it will not reuse the results of Workspace Feature Spelling and Grammar Checking for other customers. Google states in the public Workspace Data Protection Guide: "*It is important to highlight that your Customer Data is not used to improve spelling & grammar services for other customers' accounts*."[5]

In reply to this finding, Google confirmed that the Smart Features are part of the Core Services, and governed by the data processor terms. According to Google, this ensures that there is no privacy risk in use of these features.

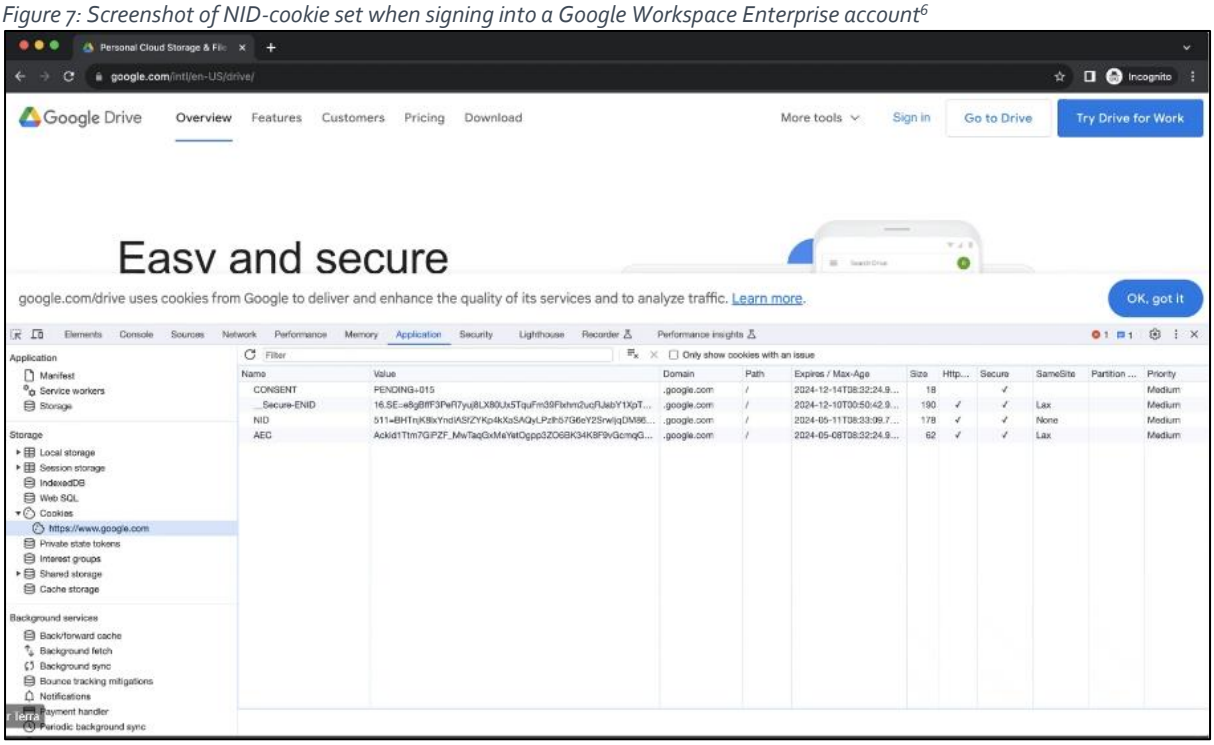
Conclusion: no high risk resulting from use of the processor-service Smart Features
Google has clarified its role as data processor for the processing of personal data from Smart Features, within the boundaries of the negotiated data processing terms. Dutch Workspace Enterprise users are free to use these services, without any additional data protection risks.

Finding 3: Use of the NID-cookie

When a Workspace Enterprise user logs-in, Google sets a NID-cookie without any user choice to accept or refuse the cookie. See Figure 8 below. Google also uses a NID-cookie when a Workspace user looks up relevant legal information from Google in the Google Cloud Privacy Notice without offering the user an option to refuse the cookie. These two issues are discussed separately below.

Use of NID-cookie in Workspace applications

Figure 7: Screenshot of NID-cookie set when signing into a Google Workspace Enterprise account[6]



[5] Google Workspace for Education data protection implementation guide, Google Whitepaper, March 2021, p. 7, URL: https://services.google.com/fh/files/misc/google_workspace_edu_data_protection_implementation_guide.pdf .

[6] Screenshot made 16 November 2023, video of the process shared with Google on 8 January 2024.

In its public cookie statement, Google explains that it uses the NID-cookie for four purposes: (i) for functional purposes, to remember setting choices, (ii) analytics, (iii) to show ads to logged-out users, and (iv) for personalization.[7]

Google writes: "*Some cookies and similar technologies are used to maintain your preferences. For example, most people who use Google services have a cookie called 'NID' or '_Secure-ENID' in their browsers, depending on their cookies choices. These cookies are used to remember your preferences and other information, such as your preferred language, how many results you prefer to have shown on a search results page (for example, 10 or 20), and whether you want to have Google's SafeSearch filter turned on. Each 'NID' cookie expires 6 months from a user's last use,* (...)."[8]

And:

"*Google services also use 'NID' and '_Secure-ENID' cookies on Google Search, and 'VISITOR_INFO1_LIVE' and '__Secure-YEC' cookies on YouTube, for analytics."*[9]

And:

"*The 'NID' cookie is used to show Google ads in Google services for signed-out users,"*[10]

And:

"*And the 'NID' cookie enables personalized autocomplete features in Search as you type search terms. These cookies expire 6 months after a user's last use.*"[11]

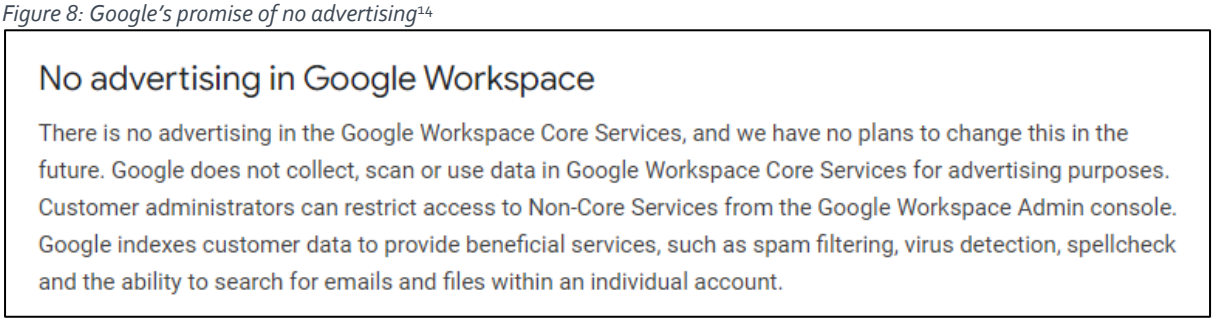
It follows from these explanations from Google that the NID-cookie is a so-called quadruple-use cookie, with a unique identifier. Google can use this unique identifier to recognise the specific browser profile (including corresponding cookie jar) of a user, until the NID cookie is deleted. Google currently uses the NID-cookie to show ads in Google services (such as YouTube and Search) for signed-out users. Earlier, Google also used the NID-cookie to show ads on third-party websites (AdSense for Search), but Google no longer uses the NID-cookie for this purpose.[12] When Google uses the NID-cookie for the purpose of following a specific browser profile (including the corresponding cookie jar) across sites, , it is a tracking cookie. Based on the Dutch implementation of the ePrivacy Directive, the reading of such a cookie requires consent.

In reply to this finding, Google has explained it does not use the NID-cookie inside Workspace Enterprise for advertising purposes, as guaranteed in Google's public security whitepaper .[13]

---

[7] Google Cookie Policy, undated, URL: https://policies.google.com/technologies/cookies?hl=en-US . Search for 'NID'.
[8] Idem.
[9] Ibid.
[10] Ibid.
[11] Ibid.
[12] Google, AdSense for Search and other Search Ads products to use new serving domains and deprecate ad personalization 3 November 2023, URL: https://support.google.com/adsense/answer/14201307?hl=en.
[13] Google Workspace Security Whitepaper, Data Usage, URL: https://workspace.google.com/learn-more/security/security-whitepaper/page-6.html .

Figure 8: Google's promise of no advertising[14]



Google also explained it will not use the NID-cookie set in Workspace for advertising purposes on external (third party) websites if the user has not provided consent for non-essential cookies. Google has technical and contractual measures to enable compliance by third parties using its advertising services with the legal consent requirement for non-essential cookies in the EU. Google's EU user consent policy requires websites that carry Google advertising to obtain consent to both the use of the NID cookie for advertising purposes on the third-party website and (if they wish to use Google's advertising services for the purpose of personalised advertising) the use of personal data for personalised advertising before calling Google's advertising services. Google enforces its EU user consent policy through a combination of audits and technical means. In May 2023, Google published a blog about stricter consent requirements for the use of its publisher-facing advertising services, including AdSense.[15]

If a Workspace Enterprise user visits a Google website such as google.com (for which Google is a data controller), the user is automatically treated as a signed-out user and google.com will present a cookie consent banner to the user. If the user does not give consent for non-essential cookies, Google cannot use the NID-cookie set in the Workspace environment and the information associated with this NID-cookie to inform advertisements on google.com.

Similarly, Google's addition of the analytical purpose to the NID-cookie does not breach the privacy of government workspace, as Google has contractually agreed not to use any Content or Diagnostic Data (including Website Data) from the Dutch Workspace Enterprise users for data analytics unless explicitly authorised by the agreement. If the NID-cookie is set when logging in to Workspace Enterprise, Google remains bound to these contractual limitations even when the end user logs out of Workspace and continues to surf to other websites where Google can read the NID-cookie.

As mentioned above, pursuant to the Dutch implementation of the ePrivacy Directive, only analytical cookies with no or little impact on privacy are exempted from the consent requirement. This exception does not apply to analytics across multiple websites.

Use of NID-cookie when reading Google Cloud Privacy Notice (GCPN)

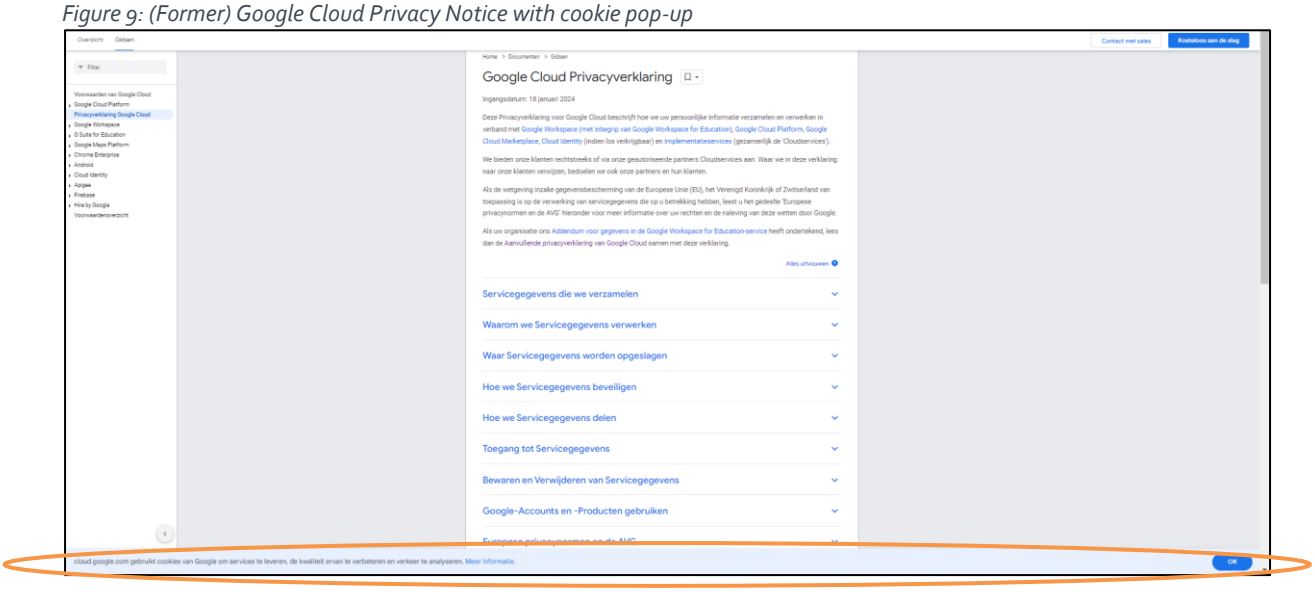
Google also uses the NID-cookie when a user wants to read the legal information in the GCPN. Privacy Company observed the use of the NID-cookie during the sign-up process for a Google Workspace account. A test user clicked on the hyperlink to this text in the pop-up screen with the terms of the new account. At that point, Google displays a banner with a question about cookies.

Initially, Google's cookie pop-up included a choice between More information or OK, without an option to refuse. See Figure 9 below.

---

[14] Google Workspace for Education, in Dutch: *Veelgestelde vragen over privacy en beveiliging*, URL: https://edu.google.com/why-google/privacy-security/frequently-asked-questions/ .
[15] Google AdSense, New Consent Management Platform requirements for serving ads in the EEA and UK. URL: https://blog.google/products/adsense/new-consent-management-platform-requirements-for-serving-ads-in-the-eea-and-uk/ .

Figure 9: (Former) Google Cloud Privacy Notice with cookie pop-up



The user was treated as logged-out user by Google. This means Google acted as a data controller, rather than a processor, for the processing of personal data through cookies.

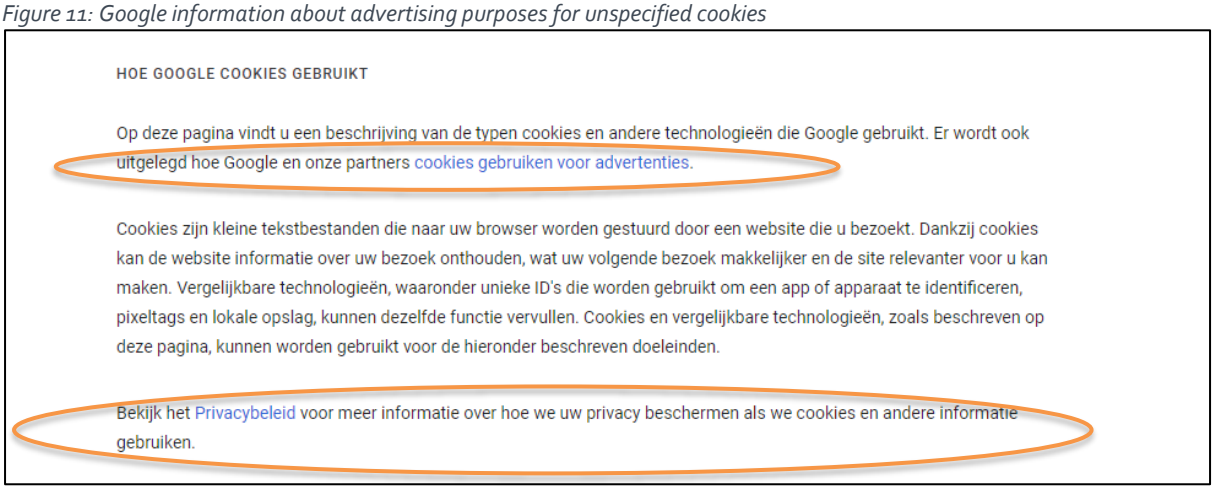
In reply to this finding, Google has confirmed that it only uses cookies on this GCPN page to offer and improve the quality of its services and to analyse traffic. Google does not use the NID cookie on the GCPN page for advertising purposes. Google launched a new version of this cookie banner on 1 February 2024, and a further redesigned banner on 13 May 2024.See Figure 10 below.

In the new version Google has changed the wording of the 'OK' button to 'I understand' to prevent the impression that Google asks for consent.

Figure 10: Google new cookie banner on GCPN page since 13 May 2024 (Dutch version)

Google now mentions 3 processing purposes in this banner: (1) to provide services, (2) to improve the quality of the services, and (3) to analyse traffic. Google also explicitly excludes the use of the NID-cookie for advertising purposes ("*Deze website maakt geen gebruik van cookies voor advertenties"*). This purpose limitation is extremely important, because Google does mention advertising in the text shown to users when they click on 'More Information'. In this paragraph Google describes it can use cookies and other unique identifiers for advertising purposes. See Figure 11 below.

Figure 11: Google information about advertising purposes for unspecified cookies


HOE GOOGLE COOKIES GEBRUIKT

Op deze pagina vindt u een beschrijving van de typen cookies en andere technologieën die Google gebruikt. Er wordt ook uitgelegd hoe Google en onze partners cookies gebruiken voor advertenties.

Cookies zijn kleine tekstbestanden die naar uw browser worden gestuurd door een website die u bezoekt. Dankzij cookies kan de website informatie over uw bezoek onthouden, wat uw volgende bezoek makkelijker en de site relevanter voor u kan maken. Vergelijkbare technologieën, waaronder unieke ID's die worden gebruikt om een app of apparaat te identificeren, pixeltags en lokale opslag, kunnen dezelfde functie vervullen. Cookies en vergelijkbare technologieën, zoals beschreven op deze pagina, kunnen worden gebruikt voor de hieronder beschreven doeleinden.

Bekijk het Privacybeleid voor meer informatie over hoe we uw privacy beschermen als we cookies en andere informatie gebruiken.

Because Google does not provide a specific explanation in this text what cookies it uses for what purposes, with what retention period, but instead describes all possible purposes, and refers to its general (consumer) Privacy Policy, users cannot know what cookies and information Google will read, and for what purposes Google will use these personal data. The French data protection authority CNIL has issued (and upheld) two fines of 100 and 50 million euro for Google's lack of offering an option to withdraw consent and the lack of a 'refuse all cookies' banner in Search and on YouTube.[16] The CNIL explicitly warned that closure of this sanction procedure does not exclude future enforcement, in particular with regard to "*the classification of cookies exempted from consent and the requirement to provide "clear and complete" information or the requirement to collect consent for each purpose.*"[17]

The purpose of 'improving the quality' of a service is too broad to qualify as strictly necessary processing, and hence, exemption from the consent requirement. In its Privacy Policy Google mentions it can use content data from users for improvement of features of its services: "*we use your information to make improvements to our services — for example, understanding which search terms are most frequently misspelled helps us improve spell-check features used across our services.*"[18] In another example, Google combines 'improvement' with 'personalisation' and 'advertising': "*Depending on your account settings, your activity on other sites and apps may be associated with your personal information in order to improve Google's services and the ads delivered by Google* [underlining added by Privacy Company]." These examples show that at least one of these 3 purposes is not well-defined.

Due to the improved wording in the banner, and the exclusion of advertising purposes, the 'quality improvement' purpose has been narrowed down.

Conclusion: high risk mitigated

Google has redesigned the cookie banner on the GCPN page to commit to users it won't use the NID-cookie for advertising purposes. This measure mitigates the high risk of the lack of a legal ground for government organisations due to Google's lack of information.

Finding 4: Content Data in telemetry

When the original DPIA and the update DPIA were written, it was not (yet) possible to separately examine the Telemetry Data collected by Google. One of the agreed improvement measures was the development of a telemetry viewer, in addition to more comprehensive public documentation on the nature of the personal

[16] CNIL press release, Closure of the injunction issued against Google, 1 August 2023, URL: https://www.cnil.fr/en/closure-injunction-issued-against-google.
[17] Idem.
[18] Google Privacy Policy, URL: https://policies.google.com/privacy?hl=en .

data collected with telemetry. For this verification review, Privacy Company used Google's new telemetry viewer (DIT, abbreviation of Diagnostic Information Tool). Inspection of these data revealed that Google collects Content Data from the spelling and grammar checker, and some directly identifiable personal data in some telemetry events (the name of an accessory). This was surprising, but Google explained convincingly why the data collection about use of the spelling and grammar checker was necessary (see below for more details). In response to this report, Google also found the collection of the (directly identifying) name of the accessory was not necessary, and Google agreed to stop collecting that name. As described in the 13 November 2023 version of the Update DPIA report, in June 2023 Google has significantly expanded its documentation about Telemetry Data. The information page about the Diagnostic Information Tool (DIT)[19] contains two sources of information: a general description with non-exhaustive examples of telemetry events[20], and detailed examples with the full payload of a representative browser telemetry event for each Workspace Core Service.[21]

Google does not offer Workspace users and administrators a choice between local or cloud-based spelling services: depending on the (internet) conditions, Google chooses a local or cloud spelling service.

In a separate section about Spelling and grammar suggestions in the telemetry data, Google publicly explains that collection through telemetry is necessary because Google allows users to work with documents and emails offline. The only way for Google to still collect input about the chosen spelling suggestions is to send that information to Google via telemetry messages the moment a user comes back online.

Google also explains that it does not retain these data longer than 1 month: "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."[22]

Google is contractually bound to collect and process only those personal data that are necessary for the agreed purposes.

Conclusion: High risk mitigated by transparency on telemetry data
By improving the transparency about this data processing, and by committing to a short retention period, Google has mitigated the high risk of a lack of control for the government organisations.

Finding 5: Scanning for child abuse material (CSAM)

When the update DPIA was drafted, it was unclear what Google's policy was with regard to automated scanning of Workspace content for child sexual abuse material (CSAM).

While there is a temporary exception in the ePrivacy Directive to the ban on the scanning of the content of communications, a positive legal obligation has not yet been adopted at European level. In May 2022 the European Commission published a proposal for a Regulation that would legally require designated providers to scan for CSAM (i.e. almost a year after the Update DPIA was finalised).[23] The EDPB and the EDPS have adopted a critical joint opinion on this proposal on 28 July 2022.[24]

---

[19] Google, Diagnostic Information Tool, URL: https://support.google.com/a/answer/12830816
[20] Idem, 'Understand your search results'
[21] Ibid.
[22] Idem, https://support.google.com/a/answer/12830816#zippy=%2Cspelling-and-grammar-suggestions
[23] European Commission, Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, COM(2022) 209 final.
[24] EDPB-EDPS, Joint Opinion 04/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, Adopted on 28 July 2022, URL: https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-042022-proposal_en.

The proposed Regulation has been scrutinised by civil society, human rights experts, cryptographers and many online service providers because the proposal required providers of operating systems and providers of communication services to build a back-door in the services that would allow for the scanning of data before they were encrypted with End-To-End-Encryption (E2EE). Aside from this controversial obligation for Client Side Scanning, the proposed Regulation also proposes that scanning may only be done by a European centre of expertise (yet to be established), in cooperation with national hotlines, and thus not by and in cooperation with the US NGO that Google is now working with: NCMEC.

The data protection authorities distinguish between the scanning of 'known' material with hashes, and detection of as yet unknown material. The data protection authorities warn that the infringement of scanning for unknown material on the fundamental rights of data subjects (such as protection of privacy, confidentiality of communications and freedom of expression) is neither necessary nor proportionate. "*As regards the necessity and proportionality of the envisaged detection measures, the EDPB and EDPS are particularly concerned when it comes to measures envisaged for* ***the detection of unknown child sexual abuse material ('CSAM')*** *and solicitation of children ('grooming') in interpersonal communication services. Due to their intrusiveness, their probabilistic nature and the error rates associated with such technologies, the EDPB and EDPS consider that the interference created by these measures goes beyond what is necessary and proportionate* [emphasis added by Privacy Company]".[25]

The EDPB and EDPS call on the Commission to explicitly prohibit voluntary scanning in the new Regulation: "Given that the detection obligations introduced by the Proposal would apply only to recipients of detection orders, it would be important to make clear in the text of the proposed Regulation that the voluntary use of technologies for the detection of CSAM and solicitation of children remains permitted only inasmuch as it is allowed under the e-Privacy Directive and GDPR. This would entail, for instance, that providers of number-independent interpersonal communications services would be prevented from using such technologies on a voluntary basis, unless this would be permitted under the national laws transposing the e-Privacy Directive, in accordance with Article 15(1) of the e-Privacy Directive and the Charter."[26] The DPAs also indicate that they see no room for scanning on a voluntary basis after the Regulation comes into force: "*For instance, the EDPB and EDPS recommend making clear that the proposed Regulation would not provide for a lawful basis for the processing of personal data for the sole purpose of detecting online child sexual abuse on a voluntary basis.*"[27]

In light of this explanation from the DPAs, SLM Rijk asked Google to explain that it only scans for known CSAM, and does not deploy machine learning (not itself, but also not indirectly through a partner like NCMEC) to discover new cases. Google unequivocally confirmed that it does not scan for unknown CSAM.

Conclusion: High risk mitigated by statement Google

Google's statement that it only scans for known CSAM, and that it does not (indirectly) use machine learning to discover new materials mitigate the potential high risk of scanning for unknown materials.

[25] Idem, Summary, p. 5.
[26] Idem, par. 20.
[27] Idem, par. 21.