



DPIA Google G Suite Enterprise

Data protection impact assessment on the processing of personal data on 3 platforms with the Chrome browser and as installed apps

Version 1 – for consultation with the Dutch DPA

Date	9 July 2020, with update on 12 February 2021
Status	Confidential

Colophon

DPIA by	Ministry of Justice and Security Strategic Vendor Management Microsoft (SLM Microsoft Rijk) Turfmarkt 147 2511 DP The Hague PO Box 20301 2500 EH The Hague www.rijksoverheid.nl/jenv
Contact	Paul van den Berg E p.j.van.den.berg@minjenv.nl T 070 370 79 11
Project name	DPIA report data processing in Google G Suite Enterprise (now: Google Workspace)
Appendix	Technical analysis data traffic
Authors	Privacy Company Sjoera Nas and Floor Terra, senior advisors www.privacycompany.eu

CONTENTS

COLOPHON	3
SUMMARY	1
INTRODUCTION	8
PART A. DESCRIPTION OF THE DATA PROCESSING	17
1. THE PROCESSING OF PERSONAL DATA	17
1.1 <i>Customer Data</i>	18
1.2 <i>Diagnostic Data</i>	18
1.3 <i>Functional Data</i>	19
1.4 <i>G Suite Core Services, Google Account, Support Services, Additional Services, and Other related services</i>	20
1.5 <i>The enrolment framework for G Suite Enterprise</i>	34
2. PERSONAL DATA AND DATA SUBJECTS	36
2.1 <i>Definitions of different types of personal data</i>	36
2.2 <i>Diagnostic Data</i>	39
2.3 <i>Outgoing traffic analysis</i>	44
2.4 <i>Results access requests</i>	48
2.5 <i>Types of personal data and data subjects</i>	52
3. DATA PROCESSING CONTROLS	54
3.2 <i>Privacy controls administrators</i>	62
4. PURPOSES OF THE PROCESSING	68
4.1 <i>Purposes government organisations</i>	68
4.2 <i>Purposes Google</i>	69
4.3 <i>Purposes Additional Services and Google Account, when not used in a Core Service</i>	76
4.4 <i>Specific purposes Chrome OS and the Chrome browser</i>	78
5. PROCESSOR OR (JOINT) CONTROLLER	79
5.1 <i>Definitions</i>	80
5.2 <i>Data processor</i>	80
5.3 <i>Data controller</i>	82
5.4 <i>Joint controllers</i>	89
6. INTERESTS IN THE DATA PROCESSING	91
6.1 <i>Interests of the Dutch government organisations</i>	91
6.2 <i>Interests of Google</i>	92
6.3 <i>Joint interests</i>	93
7. TRANSFER OF PERSONAL DATA OUTSIDE OF THE EEA	94
8. TECHNIQUES AND METHODS OF THE DATA PROCESSING	97
8.1 <i>Anonymisation</i>	98
9. ADDITIONAL LEGAL OBLIGATIONS: E-PRIVACY DIRECTIVE	100
10. RETENTION PERIODS	104
10.1 <i>Customer Data</i>	104
10.2 <i>Diagnostic Data</i>	104
PART B. LAWFULNESS OF THE DATA PROCESSING	107
11. LEGAL GROUNDS	107
11.1 <i>Customer Data from the Core Services, Features and the Google Account used in the Core Services</i>	108
11.2 <i>Personal data in Additional Services, Other related services, Technical Support Services and all Diagnostic Data</i>	116
11.3 <i>Google's own legitimate business purposes</i>	118
12. SPECIAL CATEGORIES OF DATA	119
12.1 <i>Transfer of special, sensitive, secret and confidential data to the USA</i>	120
13. PURPOSE LIMITATION	121

14.	NECESSITY AND PROPORTIONALITY.....	123
14.1	<i>The principle of proportionality.....</i>	123
14.2	<i>Assessment of the proportionality</i>	123
14.3	<i>Assessment of the subsidiarity</i>	126
15.	DATA SUBJECT RIGHTS	127
15.1	<i>Legal framework and contractual arrangements between government organisations and Google.....</i>	127
15.2	<i>Right to information.....</i>	127
15.3	<i>Right to access.....</i>	128
15.4	<i>Right of rectification and erasure.....</i>	130
15.5	<i>Right to object to profiling</i>	130
15.6	<i>Right to data portability.....</i>	131
15.7	<i>Right to file a complaint.....</i>	131
	PART C. DISCUSSION AND ASSESSMENT OF THE RISKS	132
16.	RISKS	132
16.1	<i>Identification of Risks</i>	132
16.2	<i>Assessment of Risks.....</i>	134
16.3	<i>Summary of risks</i>	147
	PART D. DESCRIPTION OF RISK MITIGATING MEASURES	149
17.	RISK MITIGATING MEASURES.....	149
17.1	<i>Measures against the ten high risks.....</i>	149
17.2	<i>Measures against the three low risks.....</i>	152
17.3	<i>Conclusions July 2020.....</i>	153
17.4	<i>Google measures 12 February 2021.....</i>	153
	<i>Risk mitigating measures taken by Google</i>	155

OVERVIEW OF FIGURES AND TABLES

Figure 1: Customer Data, Functional Data and Diagnostic Data	17
Figure 2: Different devices, OS and services in scope of this DPIA	21
Figure 3: Overview of Core Services shown in the Enterprise admin console	23
Figure 4 Features: Spellchecker, Explore, and Translate	24
Figure 5: Using <i>Spelling and grammar</i> in G Suite Docs	24
Figure 6: Welcome notice	27
Figure 7: Chrome basic spellchecker	30
Figure 8: Chrome enhanced spellchecker	31
Figure 9: Google warning to administrators when they ask for Support	33
Figure 10: Feedback	34
Figures 11 and 12: Google list of different audit logs and reports API	40
Figure 13: Example of Token audit log	42
Figure 14: G Suite Reports API: export Gmail actions	43
Figure 15: contents of sentence sent to Google Play	45
Figure 16: Google Account home screen, four controls for end users	55
Figure 17: left bar options Google Account	56
Figure 18: Information about Google Account permissions for end users	56
Figure 19: Viewing and controlling third party app access	57
Figure 20: Web & App Activity disabled by default	59
Figure 21: Location History disabled by default	59
Figure 22: Google Ad Settings for Ad personalisation	60
Figures 23 and 24: Default settings Chrome browser	61
Figure 25: Default setting: automatic release of new features	63
Figure 26: Admin overview of 51 additional Google services and Marketplace apps	63
Figure 28: Default settings Marketplace: all access is allowed	66
Figure 29: Default setting: unrestricted access to Customer Data	67
Figure 30: Changing access rights per app from full access to limited acces	67
Figure 31: Screenshot provided by Google	74
Figure 32: Google table data region selection	95
Figure 33: Google map with datacentres	96
Table 1: Comparison Core Services with Microsoft Office 365 for the Web services	11
Table 2: Platform, device and browser specifications	14
Table 3: Available Core Services included in G Suite Enterprise	22
Table 4: Tested Additional Services G Suite Enterprise	27
Table 5: 53 Additional Services	28
Table 6: Google 92 additional consumer services in the new Terms	29
Table 7: Drive Audit log	41
Table 8 Overview of individual end user actions in Gmail	42
Table 9: Google overview of self-service tools for end users	50
Table 10: Purposes Customer Data and Diagnostic Data Core Services	74

Summary

Google’s G Suite Enterprise contains communication, productivity, collaboration and security tools. In December 2020, after completion of this report, Google has renamed these services in Google Workspace.

Google provides these software services as a cloud service. Users can access the different tools through a browser or through installed apps on mobile phones and devices. This report examines the data protection risks of the use of G Suite Enterprise (for large organisations and companies) via the Chrome browser on the following 3 platforms: ChromeOS (on a Chromebook), mac OS and Windows 10. Additionally, the risks are assessed of the use of installed iOS and Android G Suite apps.

Though most government organisations use Microsoft Office 365, SLM Microsoft Rijk (the Dutch government’s department managing strategic vendor relations with Microsoft) wishes to assess via this DPIA what the risks are if government organisations would deploy G Suite Enterprise instead of Microsoft Office 365.



Within G Suite there is a fundamental difference between Core Services and Additional Services. This DPIA assesses all of the available Core Services, six Additional Services and 3 other included services (Spelling and grammar, Translate and Explore). The Additional Services are: YouTube, Maps, Web and App Activity, Location History, Google Search plus (as a single Service) the Chrome OS and the Chrome browser. These services were chosen because it is assumed they are widely used, while they may process a wide variety of content and location data.

Outcome: ten high data protection risks

The outcome of this DPIA is that there are ten high data protection risks and three low data protection risks. The high risks, and mitigating measures, are shown in the table at the end of this summary.

Personal data

This DPIA is based on a legal analysis of the available documentation about G Suite Enterprise, answers from Google to detailed questions from Privacy Company and a technical examination of the data processed by Google in its log files.

In order to gain insight in the personal data that Google stores on its own cloud servers on the individual use of the G Suite Core Services, and the personal data Google collects about the use of the tested Additional Services, data subject access requests were filed as defined in Article 15 of the GDPR, after having performed scripted scenarios.

This report distinguishes between Customer Personal Data (Customer Data actively provided by G Suite Enterprise end users); Diagnostic Data (including website and cookie data) about the use of the Core and the Additional Services, and Google Account.

Purposes, roles and legal grounds

Google contractually qualifies itself as data processor for the personal data in Customer Data it processes through the Core Services in G Suite Enterprise (described as the Customer Data in this DPIA). On the other hand, Google qualifies itself as data controller for the Google Account, most of the Additional Services including Chrome OS and the Chrome Browser, the Diagnostic Data and Other related services that may send Customer Data to Google, such as Feedback and the Enhanced Spellcheck in the Chrome browser.

At the start of this DPIA, Google's role for the built-in micro services Spellchecker, Translate and Explore functionality in some of the Core Services was not clear. Google has since clarified that it acts as a data processor for these *Features*. Google has similarly explained it processes the Google Account Data as data processor as long as the end user only uses Core Services, and no Additional Services. However, at the time of completion of this DPIA these explanations were not yet contractually guaranteed.

As data processor, Google contractually guarantees not to use any Customer Data for advertising purposes, and not to show any advertising in the G Suite Core Services. Other than this exclusion, Google has refused to provide a limitative list of purposes. Google insists it only has one purpose for the processing of the Customer Data, to provide the services according to the instructions and settings from the customer. However, this is not a correct description of purposes.

Factually Google processes the Customer Data about the Core Services for 8, and possibly 20 different purposes. The purposes for the processing of the Customer Data were distilled from the G Suite Data Processing Agreement and derived from public documentation such as Google's (consumer) Privacy Policy. At the time of completion of this DPIA (in July 2020), Google did not provide any public documentation about the purposes for which it processes the Diagnostic Data, either from the Core or from the Additional Services.

If government organisations want to be able to fulfil their role as data controllers, they must be adequately informed and agree to specific and well-defined purposes. At the time of completion of this DPIA, they aren't. Google announced it would provide more information about the processing of Diagnostic Data in a future Enterprise Privacy Notice. On 12 November 2020 Google published a Google Cloud Privacy Notice with a list of purposes.

As self-qualified data controller, Google mentions at least 33 distinct purposes in its (consumer) Privacy Policy, plus additional specific purposes for the processing via Chrome OS and the Chrome browser. There is an inextricable link between the use of the Core Services, and the processing of data about the use of the Core Services. Google can only collect personal data about the individual use of its services in its role as data processor for the Dutch government organisations. Since Google processes these Diagnostic personal Data for its own purposes, Google and the government organisations have to be qualified as joint controllers. As joint controllers, government organisations need to have a legal ground to allow Google to process these personal data for these self-determined purposes.

This is not the case. Due to the lack of purpose limitation and transparency, Google and the government organisations currently don't have a legal ground for any of the

data processing. This report provides an extensive analysis why the legal grounds of consent, necessity to perform a contract, perform a task in the public interest, or for a legitimate interest cannot be relied on, not for the content, nor for the metadata.

Risks and mitigating measures

10 high risks	Measures government organisations	Measures Google
<p>Lack of purpose limitation Customer Data</p>	<p>Agree on contractual purpose limitation</p>	<p>Become a data processor. Amend contract to provide limitative list of specific and explicit purposes for the processing of specific data</p>
		<p>Exclude the data processing for any marketing, profiling, research, analytics or advertising purpose</p>
		<p>Exclude 'compatible' or 'further' processing and the 12 possible additional purposes from the (consumer) Privacy Policy</p>
		<p>Exclude processing of Customer Data to anonymise for statistics, for re-use of <i>Spelling and Grammar</i> data for machine learning</p>
		<p>Amend contract to include exhaustive list of legitimate business purposes, when Google may act as data controller</p>
<p>Lack of purpose limitation Diagnostic Data</p>	<p>Establish policies to prevent file names and path names from containing personal data</p>	<p>Become a data processor. Amend contract to provide limitative list of specific and explicit purposes for the processing of specific data</p>
	<p>Agree on contractual purpose limitation</p>	<p>Include Chrome Enterprise in G Suite Enterprise offering, or include separate 'data processor' browser with G Suite Enterprise</p>
		<p>Exclude data processing for any marketing, profiling, research, analytics or advertising purpose</p>
		<p>Amend contract to include exhaustive list of legitimate business purposes, when Google may act as data controller</p>
<p>Lack of transparency Customer Data</p>	<p>Inform employees of the possibilities for Data Subject Access Requests, access to the audit logs and self-service tools</p>	<p>Provide exhaustive and comprehensible information about the processing of Customer Data from the Core Services, the Features, the Additional Services, the Google Account, the Technical Support Services and Other related services that may send Customer Data to Google, such as Feedback and the Enhanced Spellcheck in the Chrome browser</p>
	<p>Disclose and enforce retention policy / clean up obsolete data</p>	<p>Provide tool to provide access to the contents of Customer Data in Diagnostic Data (including telemetry data and use of Features) Give a clear warning to end users about Feedback</p>

		<p>Provide exhaustive and comprehensible documentation about the embedded Features, including the categories of data and purposes of processing</p> <p>Provide exhaustive and comprehensible information to end users upon creation of a Google Account and make this information permanently accessible</p> <p>Provide exhaustive and comprehensible information and visually clarify the difference between the three different spellingcheckers</p>
Lack of transparency Diagnostic Data	Consider prohibiting the use of Chrome OS and the Chrome browser	Publish centrally accessible exhaustive and comprehensible documentation about the types and content of and the purposes for processing of Diagnostic Data, including data collected from cloud servers and telemetry events (atoms)
		Create a tool for end users and admins to view the telemetry data
		Provide exhaustive and comprehensible information to end users upon creation of a Google Account, must be permanently accessible
		Include Chrome Enterprise in G Suite Enterprise offering, or include separate 'data processor' browser with G Suite Enterprise
No legal ground for Google and gov. orgs.	Do not use G Suite Enterprise until the processing can be based on one or more legal grounds	Become a data processor and process only for authorised purposes, so government organisations can successfully invoke the legal grounds of contract, public and legitimate interest
		Comply with cookie legislation, e.g. the Dutch telecommunications Act for the telemetry and website data (Diagnostic Data)
		Amend the contract to become an independent data controller with respect to <i>gagging orders</i> from law enforcement agencies and Google's legitimate business purposes as controller (e.g. invoicing)
Missing privacy controls	Use controls when they become available	<p>Create central controls for admins to:</p> <ul style="list-style-type: none"> • Prevent the use of the <i>Enhanced Spellchecker</i> in the Chrome browser • Prevent re-use of content from <i>Spelling and Grammar</i> for machine learning] • Limit or switch <i>Off</i> the collection of telemetry data • Change the default setting for Ads Personalization to <i>Off</i> • Prohibit the use of Additional Services • Prohibit the use of Feedback for which Google does not want to become a data processor

Privacy unfriendly default settings	Where possible, change default settings until Google has implemented adequate privacy friendly settings	Turn Off Ads Personalization
		Turn Off access to Additional Services
		Change the default setting of the Chrome browser and in the Marketplace to prevent access by default [by third parties] to Customer Data.
		Provide exhaustive and comprehensible information what the data protection consequences are if end users or administrators opt-in to privacy unfriendly settings
		Allow admins to centrally prevent any opt-in from employees
One Google Account	Advise end users not to sign in with multiple Google Accounts simultaneously	Shield or protect against spill-over from enterprise to consumer environment (and vice versa)
		Provide clear warnings to end users when they leave the protected enterprise environment
	If the Chrome browser is permitted: prohibit end users from signing in with a Google Account different from the enterprise domain	Prevent any data processing via the Google Play Store beyond authorised data processor purposes
		Amend contract to provide guarantees about processing of underwater links from Core Services to Additional Services such as Translate and Maps
Lack of control sub-processors		Amend contract to include meaningful control for customer to object against subprocessors of personal data, whether included in Customer Data, data relating to the Google Account, Support Data and Diagnostic Data or otherwise processed by Google
		Become data processor for the processing of personal data in Customer Data and Diagnostic Data from the Core Services, the Features, the Additional Services, the Technical Support Services, the Google Account, Other related services that may send Customer Data to Google, such as Feedback and the Enhanced Spellcheck in the Chrome browser and only engage authorised subprocessors
No access for data subjects	Inform employees about access to the data in the available admin log files	Honour data subject access rights, including with respect to all personal data in Diagnostic Data [collected through the Core Services, the Additional Services, the Features, the Google Account, the Technical Support Services and Other related services such as Feedback and the Enhanced Spellcheck in the Chrome browser. Develop tools to allow data subjects access to personal data when they are collected.
	When available, use other tools	

There are three low data protection risks. These stem from the lack of transparency, which could make employees think they are constantly being watched, the lack of an effective removal option for historical personal data, and the fact that Google is a cloud provider and processes personal data on servers in the United States.

Three low risks	Measures government organisations	Measures Google
Chilling effects employee monitoring system	Complement internal privacy policy for the processing of employee personal data with rules for what specific purposes specific personal data in the log files may be (further) processed and analysed. This includes listing the specific risks against which the logs will be checked, and which measures the organisations will take to ensure purpose limitation	
Impossibility to delete individual Diagnostic Data	As soon as technically possible: minimise the collection of Diagnostic Data (including telemetry and website data)	Conduct audits on data minimisation and compliance with retention periods
		Data minimisation: create a control for individual deletion Diagnostic Data without deleting the Google Account
		Guarantee that data for which deletion is requested, will not be processed for any other purpose incl. anonymisation
Cloud provider: unlawful access to Customer Data and Diagnostic Data in the USA	Follow guidance from SLM Microsoft Rijk on ECJ Jurisprudence about transfer of personal data to the USA	Consider the creation of an EU cloud
		Data minimisation by improving the privacy controls

Conclusions July 2020

This DPIA shows that -at the time of completion of this report on 9 July 2020- there were 10 high and 3 low data protection risks for data subjects when government organisations decide to use G Suite Enterprise. Because of the lack of transparency and purpose limitation, Google currently does not qualify as data processor for the processing of any of the personal data it collects in and about the use of G Suite Enterprise.

As explained in this DPIA, Google and the government organisations are joint controllers, but they cannot successfully claim any legal ground for the processing, as required in Article 6 of the GDPR. Until Google becomes a data processor, not only for the personal data in Customer Data, but also for the personal data in Diagnostic Data and other data described in this report such as personal data relating to the Google Account, government organisations are advised not to use G Suite Enterprise.

Conclusion 12 February 2021

SLM Microsoft Rijk provided Google with these DPIA findings in July 2020. Between August and December 2020, SLM Microsoft Rijk and Google discussed measures to mitigate the ten high data protection risks.

Section 17 of this report contains a table with an overview of the measures taken or announced by Google in reply to the 10 high data protection risks. On 12 February 2021 Google's reply to the final table with remaining risks was added to this conclusion.

However, the use of Google Workspace as offered under the privacy amendment of the Dutch government, still leads to 8 high risks for the different categories of data subjects involved (not just employees, but all kinds of other data subjects that may interact with the Dutch government).

SLM Microsoft Rijk proceeds by engaging in a prior consultation procedure with the Dutch Data Protection Authority.

Introduction

This report is commissioned by the Microsoft Strategic Vendor Management office (SLM Microsoft Rijk¹) of the Ministry of Justice and Security. This is the first DPIA report from the Dutch government about G Suite Enterprise.

Previously, SLM Microsoft Rijk commissioned and published impact assessments about different Microsoft Office 365 and Windows 10 products and services.² The full reports with appendices are available in English, with a short summary in Dutch. The DPIA reports have been written by the Dutch privacy consultancy firm Privacy Company.³

DPIA

Under the terms of the General Data Protection Regulation (GDPR), an organisation is obliged to carry out a data protection impact assessment (DPIA) under certain circumstances, for instance where it involves large-scale processing of personal data. The assessment is intended to shed light on, among other things, the specific processing activities, the inherent risk to data subjects, and the safeguards applied to mitigate these risks. The purpose of a DPIA is to ensure that any risks attached to the process in question are mapped and assessed, and that adequate safeguards have been implemented to mitigate those risks.

A DPIA used to be called PIA, *privacy impact assessment*. According to the GDPR a DPIA assesses the risks for the rights and freedoms of individuals. Data subjects have a fundamental right to protection of their personal data and some other fundamental freedoms that can be affected by the processing of personal data, such as for example freedom of expression.

The right to data protection is therefore broader than the right to privacy. Recital 4 of the GDPR explains: "*This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity*".

This DPIA follows the structure of the DPIA Model mandatory for all Dutch government organisations.⁴

Umbrella DPIA versus individual DPIAs

Currently, most of the approximately 300.000 employees and workers in the Dutch ministries, parliament, the High Councils of state, the advisory commissions, the police, the fire department and the judiciary, as well as the independent administrative authorities use Microsoft Office 365 software.⁵ The Google G Suite Enterprise services could be a relevant alternative for Office 365, if the outcome of the DPIA is that there are no residual high risks for data subjects whose data are processed through G Suite Enterprise.

¹ SLM is the abbreviation of the Dutch words Strategisch Leveranciersmanagement Microsoft.

² URL: <https://slmmicrosoftrijk.nl/>

³ <https://www.privacycompany.eu/>

⁴ *Model Gegevensbeschermingseffectbeoordeling Rijksdienst (PIA)* (September 2017). For an explanation and examples (in Dutch) see: <https://www.rijksoverheid.nl/documenten/rapporten/2017/09/29/model-gegevensbeschermingseffectbeoordeling-rijksdienst-pia>.

⁵ These organisations can use the future volume licenses that are negotiated by SLM Microsoft Rijk with Google.

Pursuant to Article 35 GDPR, data controllers are obliged to carry out a DPIA if the processing meets two, and perhaps three, of the nine criteria set by the European Data Protection Board (EDPB), or if it is included in the list of criteria when a DPIA is mandatory in the Netherlands.⁶

If Dutch government organisations used G Suite Enterprise, this would frequently lead to data processing on a large scale. Because G Suite is a cloud service, it is inevitable that Google processes personal data about the behaviour of employees and administrators. Additionally, Google may process data about third parties when their personal data are included in for example spreadsheets, emails and documents. The data processing involves data about the communication (be it content or metadata).

Criteria EDPB

The circumstances of the data processing via G Suite Enterprise meet three out of the nine criteria defined by the EDPB:

- There is a possibility that the processing operations (via the Google cloud log files and through the security tools for system operators) lead to a systematic observation of the behaviour of employees (criterion 3);
- The processing involves data relating to vulnerable data subjects (criterion 7, both employees and other data subjects whose personal data are processed through the G Suite Enterprise services are in an unequal relationship of power with the government organisations);
- Large scale processing of data (criterion 5, the processing potentially affects all employees of a government organisation, and possibly databases with data about many citizens).⁷

Apart from that, in their Opinion on data processing at work, the European Data Protection Authorities (EU DPAs) recommend that organisations conduct a DPIA before using “office applications provided as cloud service, which in theory allow for very detailed logging of the activities of employees.”⁸

The EU DPAs mention work applications as one of the eight relevant monitoring technologies and write: “Irrespective of the technology concerned or the capabilities it possesses, the legal basis of Article 7(f) [since replaced by GDPR art. 6(1) f, addition by the authors] is only available if the processing meets certain conditions. Firstly, employers utilizing these products and applications must consider the proportionality of the measures they are implementing, and whether any additional actions can be taken to mitigate or reduce the scale and impact of the data processing. As an example of good practice, this consideration could be undertaken via a DPIA prior to the introduction of any monitoring technology.”⁹

Criteria Dutch Data Protection Authority

The Dutch Data Protection Authority mentions one other specific criterion when a DPIA is mandatory:

⁶ Dutch DPA, (in Dutch only), list of DPIA criteria published in the Staatscourant (Dutch Government Gazette) of 27 November 2019 , URL: <https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stcrt-2019-64418.pdf>

⁷ EDPB adopted Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01), 13 October 2017, URL: http://ec.europa.eu/newsroom/document.cfm?doc_id=47711

⁸ Article 29 Working Party, WP 249, Opinion 2/2017 on data processing at work, 23 June 2017, p. 13, URL: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169

⁹ Idem, p. 14.

"Communication data (criterion 13). Large-scale processing and/or systematic monitoring of communication data including metadata identifiable to natural persons, unless and insofar as this is necessary to protect the integrity and security of the network and the service of the provider involved or the end user's terminal equipment."¹⁰

This may apply to the G Suite Enterprise services, as the monitoring of communication data could be necessary to protect the integrity and security of the network.

However, in order to be able to assess the impact of the data processing and to determine whether the actual processing meets the requirement of necessity, the government organisations must first carry out a DPIA (or have it carried out). This DPIA compares the opportunities with the risks and assesses whether measures are possible and necessary to mitigate any risks.

In GDPR terms SLM Microsoft Rijk **is not the data controller** for the processing of personal data via the use of the G Suite Enterprise services. However, as central negotiator for many cloud services, SLM Microsoft Rijk has a moral responsibility to assess the data protection risks for the employees and negotiate for a framework contract that complies with the GDPR. Therefore, SLM Microsoft Rijk commissions umbrella DPIAs to assist government organisations to select a privacy-compliant deployment, and conduct their own DPIAs where necessary. Only the government organisations themselves can assess the specific data protection risks, related to the technical privacy settings, nature and volume of the personal data they process and the vulnerability of the data subjects.

This umbrella DPIA is meant to help the government organisations with the DPIA they must conduct, but this document cannot replace the specific risk assessments the individual government organisations must make themselves.

Different G Suite editions

This report refers to G Suite Enterprise services. In December 2020, after completion of this report, Google has renamed these services in Google Workspace. Google provides three different editions of G Suite: G Suite Basic, G Suite Business and G Suite Enterprise. G Suite also offers learning and collaboration tools for schools through G Suite for Education (a 'free' version) and G Suite Enterprise for Education editions.¹¹ Google also offers 'free' versions of many core applications, such as Gmail, Docs, Hangout, Forms and Slides.

One of the key differences between the free applications and G Suite Enterprise is that the institutions can select the data region to store the Customer Data at rest from certain Services. G Suite Enterprise also offers advanced administration controls such as the G Suite Security Center and Mobile Device Management for administrators (also referred to as 'admins' in this report). G Suite Enterprise includes additional functionalities, such as enhanced analytics in BigQuery, Cloud Search across G Suite information, an eDiscovery solution called Google Vault, advanced features of the communication tool Hangouts (including video conferencing) and enhanced support.

Scope of this DPIA: G Suite Enterprise

This DPIA examines the risks of the use of G Suite Enterprise via the Chrome browser on 3 platforms: ChromeOS (on a Chromebook), mac OS and Windows 10.

¹⁰ See footnote 6.

¹¹ Google, Choose your G Suite edition. Try it free for 14 days. URL: <https://gsuite.google.com/pricing.html>

Additionally, the risks are assessed of the use of installed iOS and Android G Suite apps.

Google distinguishes between four kinds of services/applications that are related to G Suite:

1. Core Services for G Suite, including Features (built-in micro cloud services);¹²
2. Google Account
3. Services described in the Complementary Product Services Summary (only Cloud Identity if purchased as a separate service, not in scope of this DPIA), and;
4. Additional Services that can be used in conjunction with the G Suite services (53 services).

The third category of services is not in scope of this report.

This report describes five categories of services that are in scope:

1. Core Services, including *Features* such as Spelling and grammar;
2. Google Account;
3. Technical Support Services
4. Additional Services, and;
5. Related services that may send Customer Data to Google, such as the Feedback form and the *Enhanced Spellchecker* in the Chrome browser.

Additional Services (like YouTube, Maps and Search) are consumer services that may be used by G Suite Enterprise end users with their Google Account but that are not part of the Enterprise offering. Google explains in its Additional Product Terms that some of these products fall under the (consumer) Terms of Service.¹³

According to Google’s new Terms of Service of 31 March 2020, Chrome and the Chrome OS are such Additional Services. The specific services are outlined in Section 1.4 of this report, *Core Services, Features, Google Account and Additional Services*. In this DPIA they are treated as a single Additional Service, because it was technically not possible to distinguish between the traffic from the OS/browser and the traffic from the Core Services apps.

Table 1 provides an overview of G Suite Core Services, compared with similar services offered by Microsoft in Office 365. There are no direct equivalents for two of the G Suite services: Jamboard (presentation tools with hardware) and Groups for Business (discussion groups), or for Microsoft’s tool Streams (internal video streaming).

Table 1: Comparison Core Services with Microsoft Office 365 for the Web services

Google	Microsoft
Docs	Word
Sheets / Forms	Excel
Slides	PowerPoint
Gmail	Outlook /Exchange Online

¹² Google, Data Processing Amendment to G Suite and/or Complementary Product Agreement (Version 2.2), definition of ‘Services’. URL: https://gsuite.google.com/terms/dpa_terms.html.

¹³ Google, Additional Product Terms, URL: https://gsuite.google.com/intl/en/terms/additional_services.html Google writes: “The Additional Products will be governed by (a) these Additional Product Terms, and (b) the Google Terms of Service located at <https://policies.google.com/terms> or any other terms of service Google may make available (as applicable, the “Terms of Service”).”

Calendar	Calendar
Sites	SharePoint
Drive	OneDrive for Business
Hangouts Chat and Meet	Teams
Google+	LinkedIn
Keep	OneNote
Tasks	To Do
Cloud Identity Management	Azure Active Directory
Device Management	Intune

This DPIA includes analysis of all 20 Core Services, six Additional Services and three Features (Spellchecker, Translate and Explore). The six Additional Services (ChromeOS and the Chrome browser as a single service, Youtube, Maps, Search, Web and App Activity and Location History) and the Features were chosen because it is assumed they are widely used, while they may process a wide variety of content and location data.

Out of scope

The following topics are outside of the scope of this DPIA:

- Consumer products, including the 'free' unmanaged version of Gmail, Drive, Chat, Calendar, Editors, Keep, and Tasks, with the exception of the Additional Services in scope of this DPIA;
- The separate (paid) Chrome Enterprise management software;
- Additional Services other than the six investigated Additional Services (See Sections 1.4.2 and 1.4.3 of this report);
- 'Other Services' described in the G Suite Services Summary and 'Complementary Product Services' described in the Complementary Product Services provided under a separate agreement; and
- Separate technical inspection of the data processing by Chrome OS and Chrome browser (See Section 1.4.3 for the explanation).

Methodology

This DPIA was conducted between December 2019 and June 2020.

This DPIA is based on multiple sources of information. Privacy Company combined a legal fact-finding strategy with a technical examination of the data processed through the use of the G Suite Enterprise.

Legal fact-finding

Privacy Company carefully reviewed all available public documentation from Google about G Suite Enterprise, including all relevant contractual documentation for EU G Suite Enterprise customers.

Privacy Company asked questions and engaged in an ongoing dialogue with representatives of Google.

Technical fact-finding: traffic interception and data subject access requests

Because G Suite Enterprise is a remote, cloud-based service, data processing takes place on Google's cloud servers. As a result, it is not possible to inspect via traffic interception how Google processes Diagnostic Data in its system generated logs about the use of the Core Services, the Additional Services, or the Google Account.

However, it is possible to inspect the log files Google makes available to administrators about interactions from end users with its cloud servers. On 26 March 2020 14 relevant log files were exported from the administrator console that contained information about the activities performed by the two test accounts. These results are described in [Appendix 1](#) with this report, and in Section 2.2 of this report.

Additionally, Privacy Company has intercepted the data traffic from the end-user test devices. When Google collects information from the end-user device (such as telemetry data), the contents of this traffic can sometimes be decoded. Additionally, conclusion can be drawn about the network endpoints of traffic from end-user devices.

In order to map the data processing in Google's log files, first a large number of test scripts was executed on Windows and MacOS and in the different installed iOS and Android apps (the Android apps tested on the Chromebook with Chrome OS). These scripts contain a selection of representative end user actions in the G Suite Enterprise Core Services.

Where possible, the test scenarios included the use of the Features *Spelling and grammar*, *Explore* (to insert images from the Web) and *Translate*. The scenarios also used the six selected Additional Services whenever possible. The scenarios were developed in order to reproduce the everyday actions of an employee of a Dutch government organisation. The scenarios were executed on 17 December 2019 (macOS), 31 January 2020 (Windows) and 3 February 2020 (iOS and Chromebook with the Android apps). Extra tests were conducted with the (paid) Chrome Enterprise management software in May 2020, to verify the differences between the Feature *Spelling and grammar* in the Core Services, and the basic and Enhanced Spellcheck available in the Chrome browser.

Privacy Company intercepted the outgoing data with software that makes it possible to inspect the content of traffic with and without TLS encryption, Mitmproxy version 5.0.1 and Wireshark (the latter only for iOS).

The Mitmproxy was used as follows:

- configure the laptop or phone to use the proxy
- start the Mitmproxy
- launch the specific mobile application
- log in with a Google Account as needed
- run the scripted scenario. Make screenshots of each step, and
- once the script is fully executed, stop the Mitmproxy.

Privacy Company saved the captured files and compared the network endpoints with the very limited information published by Google about this topic. These results are described in Section 2.3 of this report and in [Appendix 1](#) to this report.

To compare the input from the executed test scenarios with the data stored by Google as a data controller, Privacy Company sent two formal GDPR data subject access requests to Google, requesting access and a copy of the personal data relating to the two test accounts, on 4 February 2020. Google responded by email of 27 February 2020, referring the researchers to the administrator log files. These results are described in Section 2.4 of this report.

Google does not show update data or version history for the G Suite Enterprise services. This makes it difficult to compare the test results over time, as it is not clear what changes were made, and when.

Privacy Company tested the software on three platforms with the most up to date Chrome browser.

Table 2: Platform, device and browser specifications

Operating system	Chrome browser
Lenovo Chromebook S330	Mozilla/5.0 (X11; CrOS aarch64 12607.58.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.86 Safari/537.36
Chrome on macOS	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.117 Safari/537.36
Chrome on Windows 10 Business Premium	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36
Android apps tested on Chromebook	
iOS 12.3.1	

Privacy Company ensured that the research is reproducible and repeatable. This was achieved by working with written scenarios in which the number of actions is limited. There was a pause of 30 seconds between each action. Screenshots were taken of all actions. All data have been recorded.

Input from Google

In response to the findings in part A of this DPIA, Google provided clarifications. After completion of this report, Google provided further input to the table with remaining high risks. This input is added to the summary and conclusions of this report.

Where Google pointed to factual errors, these have been corrected. Where Google requested confidentiality, these requests have generally been honoured, with the exception of information that Google already publishes. As a result of the dialogue with SLM Microsoft Rijk, Google kindly agreed to allow SLM Microsoft Rijk to publish, via this DPIA, more detailed information than it initially proposed about its anonymisation techniques and retention periods, but not about the purposes of the processing. Google also insisted on confidentiality of the information about the telemetry data it collects. In these cases, the confidential information is replaced by [CONFIDENTIAL].

Google has raised four areas of concern in the report with regard to (i) the description of its commercial interests in advertising, (ii) the interaction between the Core and the Additional Services, (iii) the analysis of the purposes of the processing, and (iv) the conclusion of joint controllership.

Based on the additional information in Google's response, Privacy Company adjusted the findings with regard to (i) Google's role as data processor for the Features and (ii) the description of the relationship between the Core Services, the Features, the Additional Services and other related services (See Section 1.4.1 of this report)

Role as data processor or joint controller

Google explained that the Features *Spelling and grammar*, *Explore* and *Translate* are part of the Core Services, and thus processed under the same privacy terms as the Core Services.

With regard to the Google Account, Google explained that there is no distinction between the consumer Google Account and the G Suite Enterprise Google Account. Google noted that although end users have to accept the (consumer) Privacy Policy when creating a Google Account for their use of G Suite Enterprise, when they access

the Core Services in the G Suite Enterprise environment, Google processes the account data as processor. Only when end users access Additional Services, such as Search or Youtube, does Google process the Google Account data as data controller.

However, at the time of completion of this DPIA, Google's role as a data processor for the processing of personal data relating to the Google Account Data and the Features was not contractually guaranteed. Furthermore, Google does not act as a data processor for the Diagnostic Data collected about the use of the Core Services, the Features, the Google Account, the Additional Services and related services such as the Feedback form and the enhanced spellchecker in the Chrome browser.

Google objects against the analysis of its role as a joint controller with its customers for the Diagnostic Data (including the telemetry and the cookie/website data). This objection is reflected in the DPIA, but did not lead to a different analysis (See Section 5.4 of this DPIA).

Purposes

Google disagrees with the list of purposes identified in this report, as it considers those purposes to be examples of processing activities, and not purposes. Google states that it only has one purpose for the processing of Customer Data as data processor: "As documented in Section 5.2.1 of the G Suite DPA Google is only contractually permitted to process Customer Personal Data according to the documented instructions of our customer described in that section. This includes an overall instruction to provide the services". Google refused to provide an exhaustive list of purposes for which it processes the different categories of Diagnostic personal Data on the use of G Suite Enterprise.

At the moment of completion of this DPIA, in July 2020, Google committed to drafting a new Enterprise Privacy Notice that will provide explicit and specific purposes for which Google processes personal data that Google collects or generates that are not personal data in Customer Data. On 12 November 2020 Google published a Google Cloud Privacy Notice with a list of purposes.¹⁴

Google's interests in the use of Diagnostic Data for personalised advertising

Part A describes that Google permits itself in its (consumer) Privacy Policy to use of Diagnostic Data for advertising purposes. In the technical inspection occurrence of a DoubleClick cookie was observed during the log-in to the G Suite Enterprise Core Services. Google disagrees with the conclusion that Google has an interest in the use of Diagnostic Data for advertising purposes, and clarified that the DoubleClick cookie was a bug which since has been fixed.

Outline

This assessment follows the structure of the *Model Gegevensbeschermingseffectbeoordeling Rijksdienst (PIA)* (September 2017).¹⁵ This model uses a structure of four main sections, which are reflected here as "parts".

1. Description of the factual data processing
2. Assessment of the lawfulness of the data processing
3. Assessment of the risks for data subjects
4. Description of mitigation measures

¹⁴ Google, Google Cloud Privacy Notice, 7 December 2020, URL: <https://cloud.google.com/terms/cloud-privacy-notice>

¹⁵ The Model Data Protection Impact Assessment federal Dutch government (PIA). For an explanation and examples (in Dutch) see: <https://www.rijksoverheid.nl/documenten/rapporten/2017/09/29/model-gegevensbeschermingseffectbeoordeling-rijksdienst-pia>

Part A explains the data processing by the different G Suite Enterprise services on the different platforms (as mobile apps and webbased, accessed via a Chrome Browser on macOS, Windows 10 and on a Chromebook). Part A starts with a technical description of the collection of the data, and describes the categories of personal data and data subjects that may be affected by the processing, the purposes of the processing, the different roles of the parties, the different interests related to the processing, the locations where the data are stored and the retention periods. In this section, factual contributions and intentions from Google are included.

Part B provides an assessment (by Privacy Company, with input from the Ministry of Justice and Security) of the lawfulness of the data processing. This analysis begins with an analysis of the extent of the applicability of the GDPR and the ePrivacy Directive, in relation to the legal qualification of the role of Google as provider of the software and services. Subsequently, part B assesses conformity with the key principles of data processing, including transparency, data minimisation, purpose limitation, and the legal ground for the processing, as well as the necessity and proportionality of the processing. Part B also addresses the legitimacy of transfer of personal data to countries outside of the European Economic Area (EEA), as well as Google's compliance with the exercise of data subjects' rights.

Part C assesses the risks for data subjects, in particular with regard to the collection of Diagnostic Data, and the use of the Additional Services.

Part D assesses the measures that can be taken by Google and the individual government organisations to mitigate the risks identified in this DPIA, as well as their impact.

Part A. Description of the data processing

This first part of the DPIA provides a description of the characteristics of the personal data that may be generated and processed by Google as a result of the use of the G Suite Enterprise services.

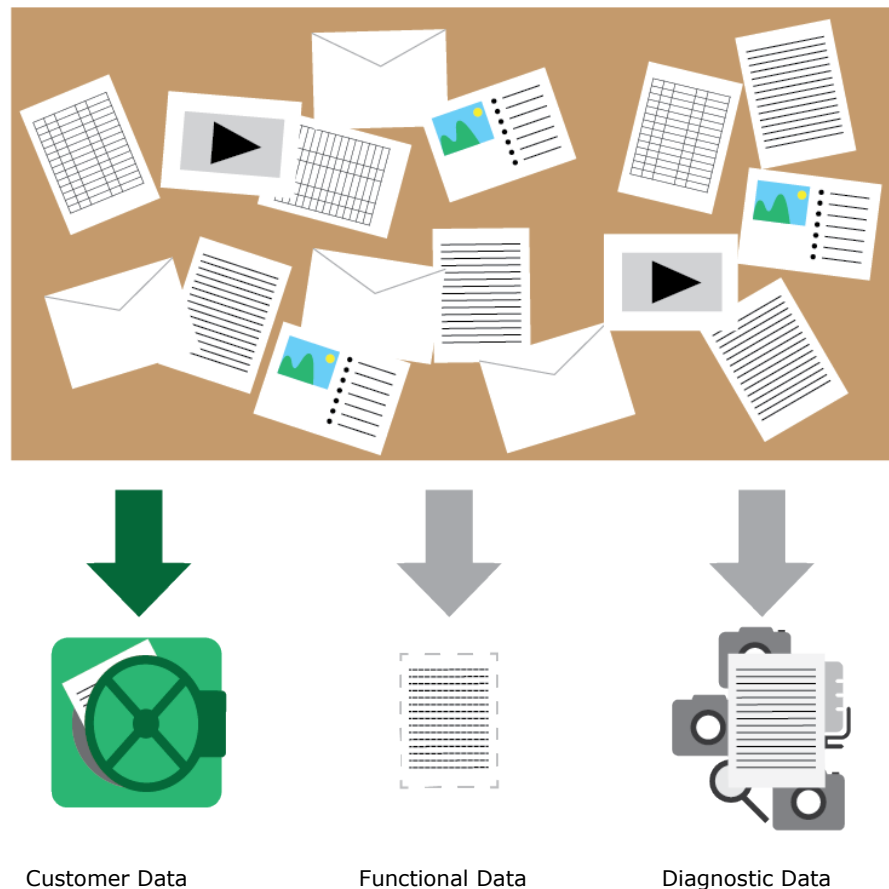
This Part A starts with a short description of the processing of different kinds of data. It continues with a description of the different categories of personal data that may be processed in the Diagnostic Data, the categories of data subjects that may be affected by the processing, the purposes of the processing by Google, the locations where data may be stored, processed and analysed, and the data protection roles of the government organisations and Google as data processor and/or as (joint) data controllers.

Finally, this part A provides an overview of the different interests related to the processing, and of the retention periods.

1. The processing of personal data

This Section 1 provides a general overview of the risks caused by the processing of personal data resulting from the use of the G Suite Enterprise service.

Figure 1: Customer Data, Functional Data and Diagnostic Data



This report distinguishes between three types of data:

1. Contents of communication with the G Suite Enterprise Core Services. Google uses the term '**Customer Data**' for all data, (including text, code, images, video and sound), provided to Google by or on behalf of government organisations or end users, but only in the Core Services;
2. **Diagnostic data**. This includes all data generated or collected by Google about the use of the Core Services in G Suite Enterprise, the Features, Google Account, Technical Support Services, Additional Services and Other related services, including telemetry and website and cookie data, only to the extent that they are stored by Google and not merely transported; and
3. **Functional data**, data that are temporarily processed to execute desired functionalities.

1.1 Customer Data

Because G Suite Enterprise is a cloud service, Google processes the contents of all files and communication from end users on its servers, such as the contents of email in Gmail, the contents of documents in Drive and the voice and audio information in teleconferencing.

Google uses the following definitions in the G Suite Data Processing Amendment:

- "Customer Data" means data submitted, stored, sent or received via the Services by Customer or End Users.
- "Customer Personal Data" means the personal data contained within the Customer Data.¹⁶

Thus, Customer Data may or may not be personal data. Examples of Customer Data that are not also personal data that may be processed through G Suite are blueprints of a building and mathematical calculations. Google explicitly limits its privacy commitments in the G Suite DPA to the personal data in Customer Data. Clause 4.1 of the G Suite DPA stipulates: "European Data Protection Law will apply to the processing of **Customer Personal Data** if, for example (...)."¹⁷

Google appears to distinguish between sensitive and less sensitive categories of personal data in Customer Data. Administrators of G Suite Enterprise may elect to store certain personal data from some Core Services System only in data centres in the European Union (EU), as described in Section 7 of this report. This extra data protection measure only applies to personal data actively provided by customers in Calendar, Drive, Forms, Gmail, Google Docs, Sheets, Slides, Hangouts Chat, New Sites and Vault. Google does not offer such a data region selection for the Diagnostic Data about the use of these or other Core and Additional Services.

1.2 Diagnostic Data

Google collects Diagnostic Data about the individual use of G Suite Enterprise services in multiple ways, for example through the use of cookies, by collecting telemetry data from the use of mobile apps and by collecting system-generated logs on its own G Suite Enterprise cloud servers. Google collects Diagnostic Data for example when end users store or access documents in Gmail, Drive, Docs and other cloud-based services. Such Diagnostic Data are stored in detailed event log files about end user activities and behaviour. These log files also contain information about the activities of the administrators.

Google mentions the following Diagnostic Data in a public privacy notice for end users of the G Suite Enterprise for Education:

¹⁶ Google Data Processing Amendment to G Suite and/or Complementary Product Agreement (Version 2.2), URL: https://gsuite.google.com/terms/dpa_terms.html

¹⁷ Idem.

- “device information, such as the hardware model, operating system version, unique device identifiers, and mobile network information including phone number of the end user;
- log information, including details of how an end user used our service, device event information, and the end user's Internet protocol (IP) address;
- location information, as determined by various technologies including IP address, GPS, and other sensors;
- unique application numbers, such as application version number; and
- cookies or similar technologies which are used to collect and store information about a browser or device, such as preferred language and other settings.”¹⁸

At the moment of completion of this DPIA, in July 2020, Privacy Company was not able to find similar public information for end users of G Suite Enterprise. Google confirmed it had not yet published a similar explanation about the processing of Diagnostic Data in the context of G Suite Enterprise. However, Google has committed to publish a new Enterprise Privacy Notice about the purposes for the processing of data other than the Customer Data.¹⁹ On 12 November 2020 Google published a Google Cloud Privacy Notice with a list of purposes.²⁰

Administrators of G Suite Enterprise have access to 19 different kinds of log files with Diagnostic Data.²¹ Fourteen of these log files contained information in the scope of this DPIA. The contents of these files are described in Section 2.2 of this report.

Google explains why the log files are useful: “As an administrator, you can examine potential security risks, measure end user collaboration, track who signs in and when, analyze administrator activity, and much more. You can view domain-level data alongside granular, user-level details through graphs and tables.”²²

As will be explained in Section 1.4.2 of this report, it is mandatory for end users of the G Suite services to create a Google Account. According to its (consumer) Privacy Policy, Google collects the following Diagnostic Data about each Google Account: “We collect information about the apps, browsers, and devices you use to access Google services, which helps us provide features like automatic product updates and dimming your screen if your battery runs low. The information we collect includes unique identifiers, browser type and settings, device type and settings, operating system, mobile network information including carrier name and phone number, and application version number. We also collect information about the interaction of your apps, browsers, and devices with our services, including IP address, crash reports, system activity, and the date, time, and referrer URL of your request.”²³

1.3 Functional Data

In this report, the term functional data is used for all data that are only necessary for a short period of time, to be able to communicate with Google’s cloud services.

¹⁸ Google G Suite for Education Privacy Notice, Information we collect, URL: https://gsuite.google.com/intl/en/terms/education_privacy.html.

¹⁹ From responses provided by representatives of Google to SLM Microsoft Rijk during the course of this DPIA.

²⁰ Google, Google Cloud Privacy Notice, 7 December 2020, URL: <https://cloud.google.com/terms/cloud-privacy-notice>

²¹ These log files are: Admin, Login, SAML –out of scope, LDAP –out of scope, Drive, Calendar, Context-Aware Access–out of scope, Devices, Password Vault–out of scope, Token, Groups, Hangouts Chat, Google+, Voice–out of scope, Hangouts Meet, User Accounts, Access Transparency-out of scope, Rules, and Email Log Search.

²² Google, G Suite Admin Help, Monitor usage and security with reports, URL: https://support.google.com/a/answer/6000239?hl=en&ref_topic=9026900

²³ Google Privacy Policy, 31 March 2020, URL: <https://policies.google.com/privacy?hl=en-US#infocollect>

Examples of such functional data are the Customer Data and the Diagnostic Data processed by an email server to deliver the communication, and the data stream necessary to allow the end user to authenticate or to verify if the end user has a valid Google Account. According to the distinction between the three categories of data made in this report, functional data may also include the content of text end users want to have translated or spellchecked. In these cases, it is necessary for Google as a cloud provider to collect the context, to provide better spelling or translation. The key difference between functional data and Diagnostic Data as defined in this report, is that functional data are and should be transient.²⁴ This means that these data should be immediately deleted or anonymised upon completion of the transmission of the communication. Otherwise they qualify as Customer Data or Diagnostic Data. As long as Google does not store these functional data, they are not Diagnostic Data.

1.4 G Suite Core Services, Google Account, Support Services, Additional Services, and Other related services

As explained in the Introduction, this report describes five key elements of the G Suite Enterprise offering.

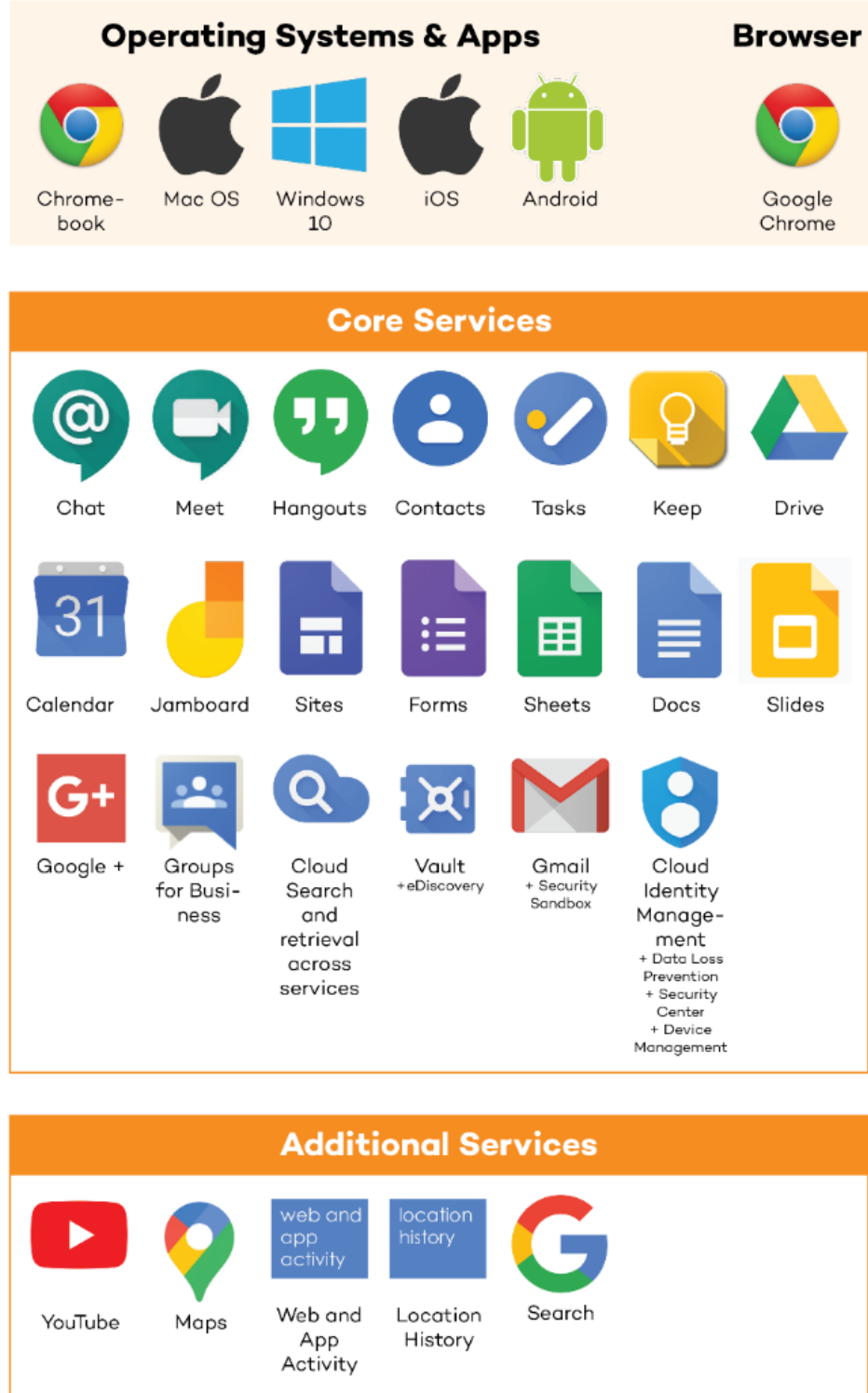
1. Core Services, including *Features* such as the Spellchecker;
2. Google Account;
3. Technical Support Services
4. Additional Services, and;
5. Other related services that may send Customer Data to Google, such as Feedback and the Enhanced Spellcheck in the Chrome browser.

Figure 2 below shows an overview of the Core Services and the Additional Services.

²⁴ Compare Article 6(1) of the EU ePrivacy Directive (2002/58/EC, as revised in 2009 by the Citizens Rights Directive) and explanation in recital 22: “*The prohibition of storage of communications and the related traffic data by persons other than the end users or without their consent is not intended to prohibit **any automatic, intermediate and transient storage** of this information in so far as this takes place **for the sole purpose of carrying out the transmission** in the electronic communications network and **provided that the information is not stored for any period longer than is necessary for the transmission and for traffic management purposes**, and that during the period of storage the confidentiality remains guaranteed.*”

Figure 2: Different devices, OS and services in scope of this DPIA

Scope Data Protection Impact Assessment G Suite Enterprise



Working Offline with G Suite Enterprise

G Suite is essentially designed to run in a browser, but some cloud applications (Google documents, sheets and slides) can also be used offline.²⁵ This requires use of the Chrome browser, and the use of the plug-in Google Docs Offline Chrome Extension. This plug-in has to be downloaded from the Additional Service Chrome Web Store. The data processing is subjected to Google’s (consumer) Privacy Policy.²⁶

Gmail has a separate option to work offline with Gmail and Calendar in a Chrome browser.²⁷ Any changes will be synced to the cloud when the end user reconnects to the Internet.

It is also possible to work offline with some of the G Suite Enterprise mobile apps and Google offers a Drive desktop client — but end users first have to check an option to download a file to their desktop or mobile device.²⁸

Access for third parties

Generally, Google delivers the Core and Additional services itself, without the help of other service providers. In other words, Google does not use third party services in its Core Services. The only exception discovered in the technical research is traffic that is sent to third party websites if a controller builds a website with the service Sites. When the developer includes content for third party websites, this logically leads to traffic to those third parties.

However, end users can of course decide themselves to share data from the G Suite Enterprise services with third parties through the use of third-party apps and by visiting websites, if permitted by the administrators.

In the test set-up of this DPIA, a Google Account used in G Suite Enterprise was used to log-in to the external filesharing platform Dropbox to test the G Suite Core Service Cloud Identity.

End users can also authorise apps to access their G Suite data when they install such apps from the Google Play app store or the G Suite Marketplace. These app stores are Additional Services. If add-ins from the G Suite Marketplace want access to the Customer Data, an end user must authorise such an app in the same way authorisations are given for the single sign-on with OAUTH or SAML. The controls for access to personal data for third parties are described in Sections 3.1 and 3.2 of this report.

1.4.1

Core Services for G Suite Enterprise including Features

As shown in Figure 3 and Table 3 below, this DPIA examines the data processing via 20 Core Services. Additionally, this DPIA assesses the risks of the data processing through Features that are embedded in the Core Services, such as *Spelling and grammar*, *Translate*, and *Explore*.

Table 3: Available Core Services included in G Suite Enterprise²⁹

Calendar	Chat
----------	------

²⁵ Google, Use Google Drive files offline, URL: <https://support.google.com/drive/answer/2375012?hl=en>

²⁶ Google, Google Docs Offline Chrome Extension, URL: <https://chrome.google.com/webstore/detail/google-docs-offline/gqbmnnjoeekpmoecnninlnbdjolhkh>

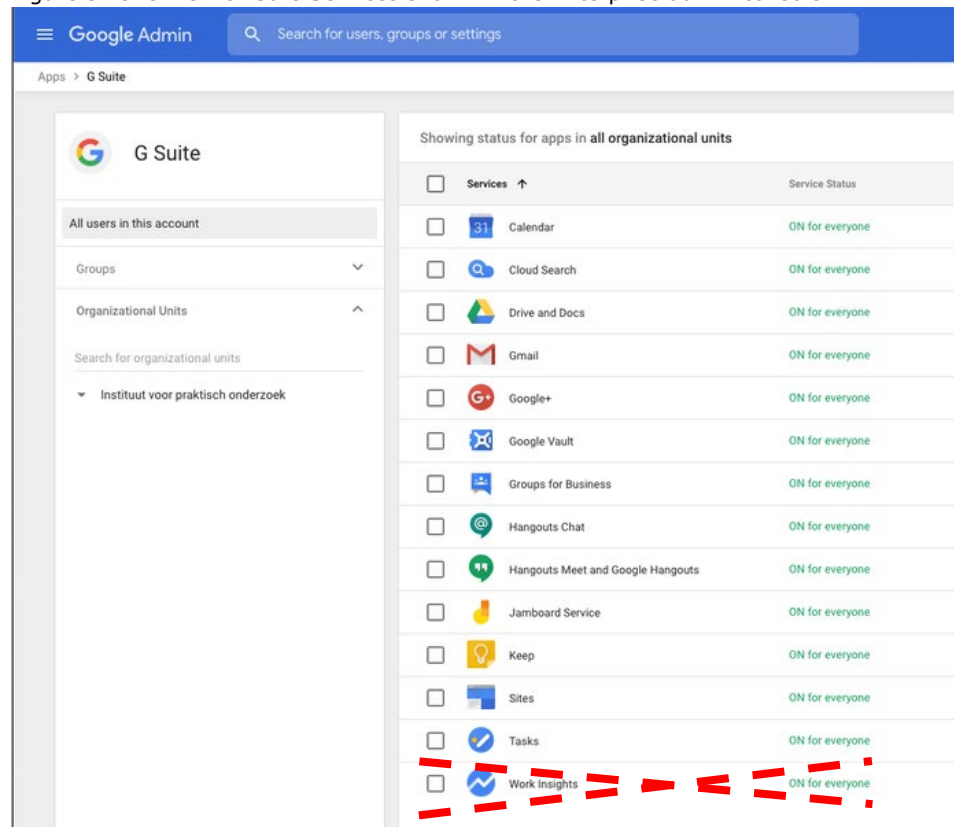
²⁷ Google, Work offline in Gmail, URL: <https://support.google.com/a/answer/7684186?hl=en>

²⁸ See footnote 23 above.

²⁹ The list includes Google+. This service is only available for G Suite Enterprise and G Suite Enterprise for Education end users.

Cloud Identity Management, including Data Loss Prevention for Gmail and Drive ³⁰ , Security Center and Device Management ³¹	Cloud Search (internal information)
Contacts	Docs
Drive	Forms
Gmail, includes Security Sandbox	Google+
Groups for Business	Hangouts
Jamboard	Keep
Meet	Sheets
Sites	Slides
Tasks	Vault, inc. eDiscovery

Figure 3: Overview of Core Services shown in the Enterprise admin console



One of the Core Services shown to G Suite Enterprise administrators is not available. Work Insights, an analytical service, is not available for customers in the EU.

Built-in Features

The Core Services include a number of Features (micro cloud services), such as the Spellchecker, shown in [Figure 4](#).

For this DPIA three of these Features were chosen to be tested:

- Explore (inserting images in documents from the web);
- Spelling and grammar; and
- Translate

³⁰ Google, G Suite Enterprise FAQ, URL: https://support.google.com/a/answer/7676757?hl=en&ref_topic=9000186

³¹ Google, G Suite Enterprise edition Premium office suite with enhanced security, controls, and customization, URL: <https://support.google.com/a/answer/7284269?hl=en>

Additionally, some Features were unintentionally included in the tests. In reply to this DPIA, Google explained that when some Additional Services such as Google Maps are embedded in the Core Services, these should also be considered as Core Services Features. The use of Calendar triggered the use of Google Maps, without any active intervention from the end user.

Features are automatically available for all G Suite Enterprise end users, and cannot be disabled by administrators. Google explains that the Spellchecker is included in Google Docs, and is based on machine learning.³² Admins cannot prevent Google from reusing the contents of spellchecked words and sentences for this purpose of machine learning.

Figure 4 Features: Spellchecker, and Translate

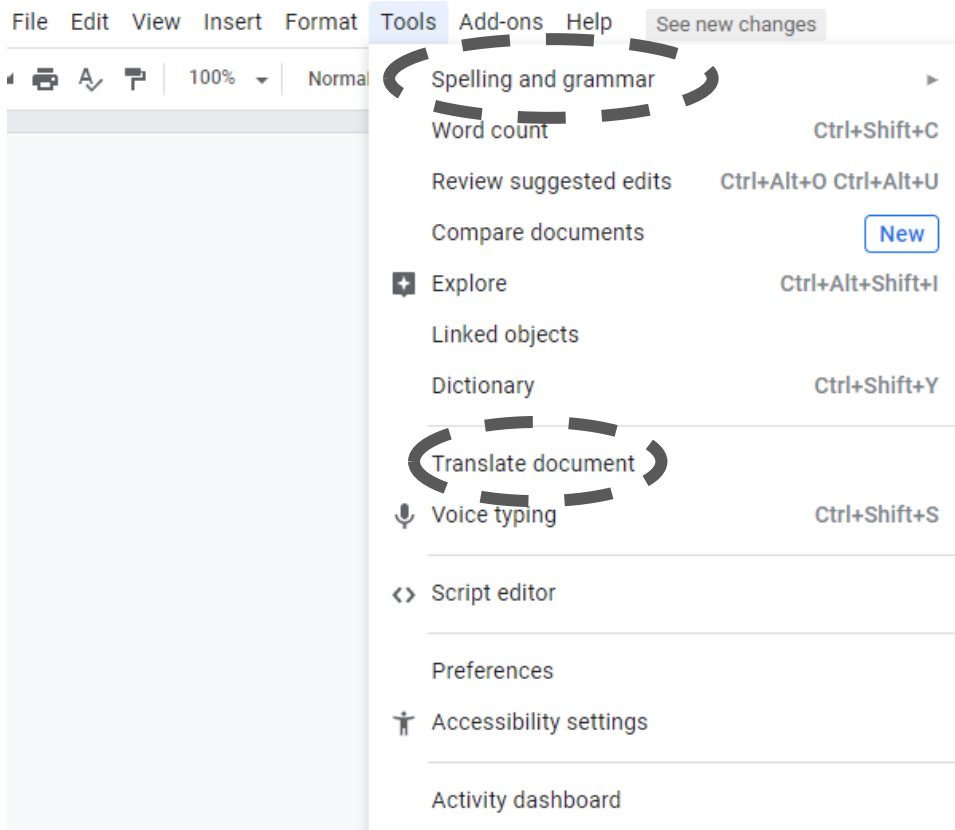
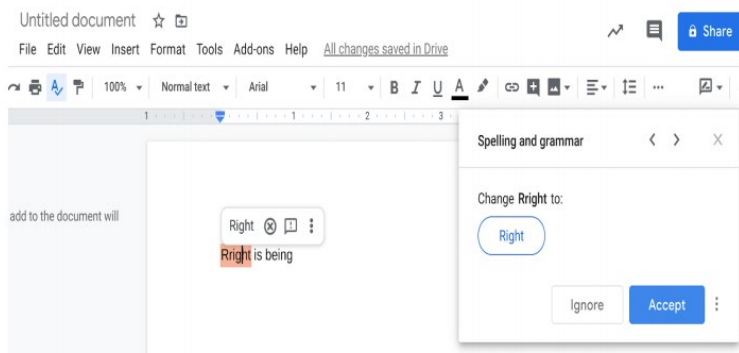


Figure 5: Using *Spelling and grammar* in G Suite Docs



³² Google, Correct your spelling & grammar in Google Docs, URL: <https://support.google.com/docs/answer/57859?co=GENIE.Platform%3DDesktop&hl=en>

Google writes:

*"Spelling suggestions are powered by machine learning. As language understanding models use billions of common phrases and sentences to automatically learn about the world, they can also reflect human cognitive biases. (...). Google is committed to making products that work well for everyone, and are actively researching unintended bias and mitigation strategies."*³³

Google explained in reply to this DPIA there are three kinds of spellchecker. In addition to the Feature *Spelling and grammar*, the Chrome browser also offers two kinds of spellchecker. There is a local (basic) Chrome Spellchecker, and the enhanced Chrome Spellchecker, which sends data to Google's cloud servers. In the G Suite Enterprise environment, admins cannot prevent their end users from using the enhanced cloud Chrome spellchecker. If they want to centrally block this traffic, they must separately procure the Chrome Enterprise service. The *Basic Spellchecker* and the *Enhanced Spellcheck* are described in Sections 1.4.1 and 1.4.4 of this report.

Explore offers end users the possibility to search images or content in third party websites, through [the Core Service] Cloud Search or on the organisational Core Service Drive.³⁴

Google explains:

*"Spellchecker Grammar Check and Explore are Core Service product features. Google is a data processor of personal data processed through use of the Spellchecker and the G Suite DPA includes the applicable privacy terms."*³⁵

Google does not publish an exhaustive list of Features, or of the applicable privacy terms. Features are similar to Additional Services (which are discussed in Section 1.4.3), because they can be used in conjunction with the Core Services. However, unlike Additional Services, Features are governed by the G Suite DPA when used in conjunction with the G Suite Enterprise Core Services.

Google offers more of such embedded Features in the Core Services. As will be detailed in Section 2.3 of this DPIA, in some test scenarios the use of a Core Service automatically triggered the use of an Additional Service. For example, when an appointment was made in Calendar, the location of the appointment was automatically searched in Google Maps. When an end user used the built-in Feature *Translate* in a document, the Additional Service *Translate* was used in the background. Google explained that when an Additional Service such as Google Maps is included as a 'Feature' of a Core Service, the personal data are anonymised before they are processed in the backend consumer infrastructure.

*"Certain Core Service product functionality shares backend infrastructure with consumer products like Translate, Maps, and Search. Google has designed strong technical separation between enterprise and consumer end users, and enterprise G Suite queries to such shared backend infrastructure are anonymised (i.e., no identifying information is processed or logged). Maps in Calendar, Translate a document, and Explore are features with these protections."*³⁶

It is not clear when use of an Additional Service is a Feature, and when not. Google explained that when an end user includes content from Youtube in a website created

³³ Ibid.

³⁴ Google, See and use suggested content in a document, URL: https://support.google.com/docs/answer/2481802?visit_id=637209012175591419-19104268&p=docs_explore&hl=en&rd=1

³⁵ Google response to part A of this DPIA.

³⁶ Google response 5 June 2020.

with the Core Service Sites, the Youtube data are not considered a Feature, and thus, not anonymised.

Google indicated its willingness to improve its public documentation about this integration.³⁷

1.4.2

Google Account

To use the G Suite Enterprise services, each end user must create a Google Account. Google processes the Google Account in its backend infrastructure for identity (including account type) and authentication purposes. Google Account also include profile data actively provided by a user.³⁸

The Google Account can be Customer Data as well as Diagnostic Data. This depends on how the end user provides information. The end user can provide information directly, when providing a name and profile picture (Customer Data), or indirectly, when Google collects information about when and for what purposes, in what context (app/web, platform and device) an end user logs in (Diagnostic Data).

In reply to questions raised during this DPIA, Google explained that there is only one type of Google Account. This means that there is no technical separation between the Google Account for its consumer services, and the account used for G Suite Enterprise. As a result, it depends on the service the end user accesses with the Google Account whether Google acts as data controller, or as a data processor.

Google wrote:

"When a G Suite end user accesses products and services outside of G Suite, the Google Privacy Policy or another applicable Privacy Policy describes how data (including your Google Account profile information) is collected and used. A G Suite administrator controls which other Google services an end user may access while logged into a Google Account managed by its organization."³⁹

Google also explained:

"We consider Google Accounts to primarily serve as engineering infrastructure by which an end user authenticates and gains access to whatever services the end user is allowed to access by virtue of its relationship with Google. Google Account is processed in the same way as Core Service data when its functionality is used in conjunction with Core Services (to which the G Suite DPA, rather than the Google Privacy Policy would apply)."⁴⁰

When creating a Google Account, Google informs the end user that he/she has to accept the Google Terms of Service and the (consumer) Privacy Policy. After clicking on the 'Accept' button (See [Figure 6](#) below) this information with the hyperlinks disappears and cannot be retrieved by the end user.⁴¹

³⁷ Idem.

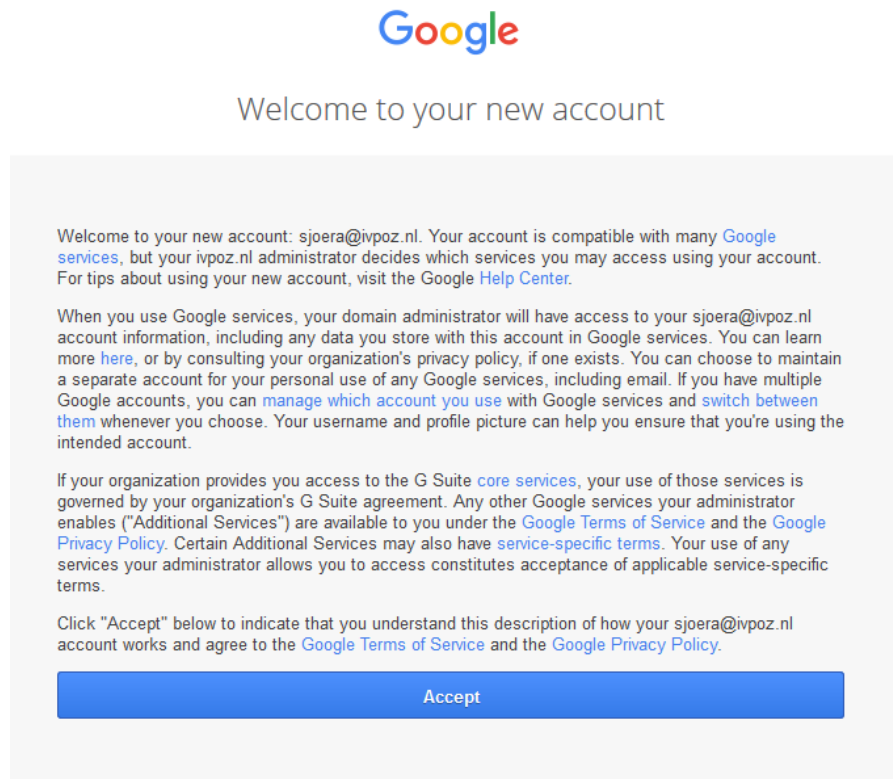
³⁸ Users can provide information about themselves such as full name, gender, birthday and picture, address and phone number through the Google Account end user interface, URL: <https://myaccount.google.com/>

³⁹ Google response 5 June 2020.

⁴⁰ Google reply to part A of the DPIA.

⁴¹ In reply to this DPIA, Google added the following information: "Links to the Privacy Policy and Terms of Service are offered directly if a user clicks on their own icon which is shown when they are in a logged in state."

Figure 6: Welcome notice



1.4.3 *Additional Services for G Suite Enterprise (including ChromeOS and the Chrome browser)*

Google explains that through the Core Services, Additional Services can be accessed for use *in conjunction with the Services*. However, these Additional Services are not part of the Core Services, do not fall under the G Suite DPA but are subject to separate 'Additional Product Terms'.⁴²

In G Suite Enterprise, all Additional Services are enabled by default. If the administrator does not restrict the use of the Additional Services, end users are not asked for consent. As shown in [Figure 6](#) above, they have to accept different terms of service, including the (consumer) Google Terms of Service, when they create a Google Account to use G Suite Enterprise at work. According to Google, it requires a direct contractual relationship with end users of products not sold under the G Suite Enterprise terms at the time of account provisioning. Google reasons that end users enter into a direct agreement with Google by accepting these terms through this Welcome notice.⁴³

For this DPIA, six Additional Services were tested, as shown in [Table 4](#) below.

Table 4: Tested Additional Services G Suite Enterprise

YouTube	Google Maps
Web and App activity	Location History
Google Search	Chrome OS and Chrome browser ⁴⁴

⁴² Google Additional Product Terms, URL: https://gsuite.google.com/intl/en/terms/additional_services.html.

⁴³ Google reply to part A of the DPIA.

⁴⁴ In this DPIA, the Chrome OS and Chrome browser are treated as a single Additional Service, because they have not been separately tested, and because they share the same separate Privacy Notice and Product Terms.

More information about these six Additional Services is provided at the end of this Section.

Google currently offers 53 Additional Services, as shown in [Table 5](#). These services can be disabled by admins. This list is dynamic. Admins can see the most current list of Additional Services in the Admin Console.⁴⁵

Table 5: 53 Additional Services⁴⁶

App Maker	Blogger	Campaign Manager
Chrome Web Store	FeedBurner	Fusion Tables
Google Ad Manager	Google Ads	Google AdSense
Google Alerts	Google Analytics	Google Bookmarks
Google Books	Google Chrome Sync	Google Classroom
Google Cloud Platform	Google Custom Search	Google Data Studio
Google Domains	Google Earth	Google Finance
Google Groups	Google In Your Language	Google Maps
Google My Business	Google My Maps	Google News
Google Partners	Google Payments	Google Photos
Google Play	Google Play Console	Google Public Data
Google Scholar	Google Search Console	Google Shopping
Google Takeout	Google Translator Toolkit ⁴⁷ (different from Google Translate!)	Google Trips
Individual Storage	Location History	Merchant Center
Mobile Test Tools	Partner Dash	Play Books Partner Center
Project Fi	Science Journal	Search Ads 360
Studio	Third-party App backups	Tour Creator
Web and app activity	YouTube	

In total, Google offers 92 different consumer services under the (consumer) Terms of Service, last updated on 31 March 2020. Since, these Terms include a link to all Google Services.⁴⁸ All these services can be accessed with a Google Account. Some of these services are Core Services in the G Suite Enterprise environment (marked in grey).

⁴⁵ <https://admin.google.com/ac/appslst/additional> .

⁴⁶ Full list of available Additional Services: Google, G Suite Additional Services, URL: <https://support.google.com/a/answer/181865?hl=en> Additionally, Google offers 'unlisted' Additional Services, *that do not have an individual control (such as Allo, Chromecast, and Google Surveys)*. Admins can decide to turn all of these services ON or OFF through the Google Admin console but have no individual controls for these services. Google, Manage services that are not controlled individually, URL: <https://support.google.com/a/answer/7646040?hl=en>

⁴⁷ On 4 December 2019, Google shut down the Translator Toolkit. See: Google, Google Translator Toolkit Has Shut Down, URL: https://support.google.com/answer/9464390?visit_id=637209012175591419-1479104268&rd=1 and 9to5 Google, 2 December 2019, Google shuts down Translator Toolkit this week after a decade, URL: <https://www.9to5google.com/2019/12/02/google-translator-toolkit-shutdown/#>

⁴⁸ Google, Services that use Google's Terms of Service and their service-specific additional terms and policies, URL: <https://policies.google.com/terms/service-specific?hl=en-GB>. The list includes services that are Core Services in the G Suite Enterprise environment, and tools that soon stop to exist (such as Google Cloudprint, see: Google, Migrate from Cloud Print, URL: <https://support.google.com/chrome/a/answer/9633006>)

Table 6: Google 92 additional consumer services in the new Terms

Android Auto	Android OS	Android TV	Authenticator
Assistant	Blogger	Book Search	Calendar
Cardboard	Chat features	Chrome and Chrome OS	Connected Home
Contacts	Contributor	Course Builder	Data Studio
Daydream View	Docs	Drawings	Drive
Files Go	Finance	Forms	Gallery Go
Gboard	Gmail	Google Alerts	Google Arts & Culture
Google Classroom	Google Cloud Print	Google Digital Garage	Google Duo
Google Earth	Google Expeditions	Google Fit	Google Flights
Google Fonts	Google for Nonprofits	Google Glass Explorer	Google Go
Google Groups	Google Input Tools	Google Lens	Google Local Services
Google Manufacturer Center	Google Merchant Center	Google My Business	Google One
Google Pay	Google Photos	Google Pixel Phones	Google Play
Google Play Books	Google Play Games	Google Play Movies & TV	Google Play Music
Google Play Protect	Google Shopping	Google Store	Google Street View
Google Tag Manager	Google Trends	Google Web Designer	Hangouts
Hangouts Chat	Image Search	Keep	Local Guides
Maps	Messages	News	Optimize
Patent Search	Personal Safety	PhotoScan	Recorder
Question Hub	Reserve with Google	Scholar	Search
Search Console	Sheets	Shopping Actions	Sites
Slides	Snapseed	Stadia	Tasks
Tilt Brush	Translate	Trips	Voice

Google Search

The term Google Search can be confusing. Google offers three types of search. In this report, 'Google Search' refers to the well-known search engine service. In addition, Google offers 'Cloud Search'. This Core G Suite Service allows organisations to search in all G Suite documents in their own organisation. Google also offers the separate Additional Service *Search and Assistant*. This service allows end users to save their search history.

Google explained:

*"Users who have the service [Search and Assistant] turned off can still use Google Search and Google Assistant without using or saving information with their account."*⁴⁹

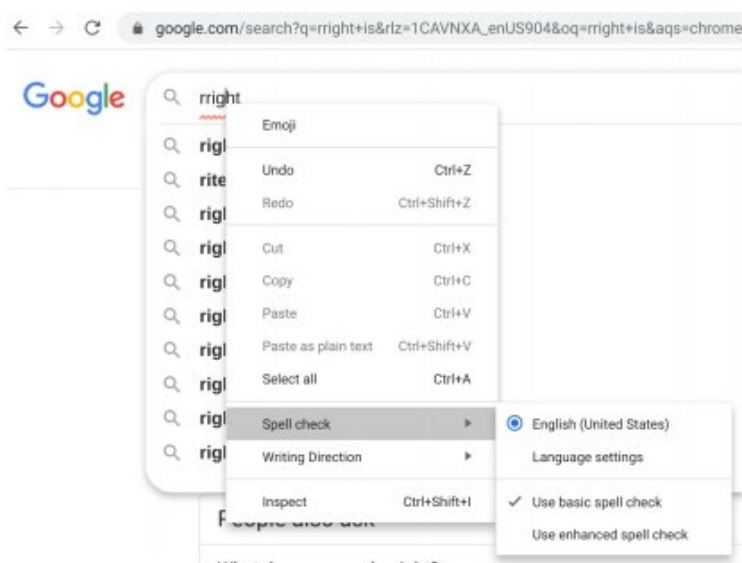
⁴⁹ Google reply to part A of the DPIA.

Chrome OS and the Chrome browser

Chrome OS and the Chrome browser are governed by Google's consumer Terms of Service, as shown in [Table 5](#), plus Additional Terms of Service⁵⁰ and a separate privacy notice.⁵¹ The Additional Terms do not contain relevant privacy information.⁵² In the separate Chrome privacy notice for the Chrome OS and the Chrome browser however, Google lists specific purposes for the processing of personal data. These will be discussed in Section 4.4 of this report.

As described in Section 1.4.1 above, there are three spellcheckers in G Suite Enterprise: the Feature *Spelling and Grammar*, which is part of the Core Services, and two spellcheckers that are available in the Chrome browser: a local *Basic Spellchecker* and a cloud *Enhanced Spellcheck*. Both of the spellcheckers in the Chrome browser are accessed with a right click on a misspelled word. See [Figures 7 and 8](#) below.

Figure 7: Chrome basic spellchecker



For the end-user, the difference with the G Suite Feature *Spelling and grammar* is not obvious. When checking the spelling of a document, the end user can use all three spellcheckers, without any clear distinction of its origin, part of a Core Service or part of the Additional Service Chrome browser.

At the time of completion of this DPIA, Google does not provide an explanation to end users what the difference is between the basic and the enhanced spellchecker available in the Chrome browser.⁵³ The *Enhanced Spellcheck* cannot be disabled by admins. Such functionality is available in Chrome Enterprise which can be purchased as a different product, governed by separate terms.⁵⁴ Thus, if admins would like to

⁵⁰ Google, Google Chrome and Chrome OS Additional Terms of Service, URL: <https://www.google.com/chrome/terms/?hl=en>

⁵¹ Google Chrome Privacy Notice, Last modified: May 20, 2020, URL: <https://www.google.com/chrome/privacy/?hl=en>

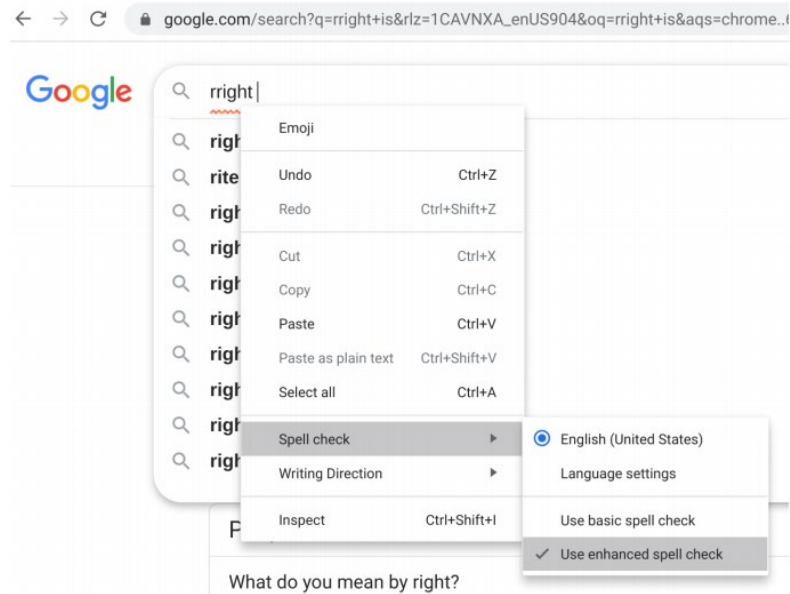
⁵² They describe the rules for the built-in Adobe functionality, mostly related to content protection.

⁵³ After completion of this report in July 2020, Google published the Google Workspace Data Protection Implementation Guide, URL: https://services.google.com/fh/files/misc/google_workspace_data_protection_guide_en_dec2020.pdf. This guide does contain an explanation of the difference.

⁵⁴ Google, Chrome Service License Agreement, URL: <https://cloud.google.com/terms/chrome-enterprise/chrome-service-license-agreement>

disable the *Enhanced Spellcheck*, they have to purchase a separate license for Chrome Enterprise.⁵⁵

Figure 8: Chrome enhanced spellchecker



In the help center for admins Google explains the difference between the Chrome browser for consumers and the Chrome browser for Enterprises: “*The Chrome Browser for the enterprise (sometimes referred to as Chrome Enterprise) is the same Chrome Browser used by consumers. The difference is in how the browser is deployed and managed. Downloading the Chrome Enterprise Bundle, IT administrators can install the Chrome Browser via MSI, and manage their organization’s Chrome Browsers via group policy to enforce over 200+ policies.*”⁵⁶

Chrome Enterprise is not included in the G Suite Enterprise contract, and is therefore out of scope of this DPIA. Privacy Company has nonetheless tested if the *Enhanced Spellcheck* can indeed be blocked with Chrome Enterprise. This is the case, as further discussed in Section 2.3 of this report.

Combinations of Core Services with Additional Services

The Core Services are sometimes linked to the use of Additional Services or share product functionality with Additional Services. Google treats those combinations of consumer and enterprise services in different ways. In Section 1.4.1 the automatic triggering of Additional Services such as Maps and Translate is discussed as part of Core Service Features. Another combination occurs with advanced device management. Admins need advanced device management for essential information security compliance. This allows them to manage iOS apps (not just Android apps), wipe devices remotely, use Android work profiles, and more.⁵⁷ If an admin wants to roll out this Core Service, end users must install a separate app on their mobile

⁵⁵ Google, Chrome Enterprise, URL: <https://cloud.google.com/chrome-enterprise>. According to an external source, the price per license per year per device would start at 50 USD. Source: <https://reviews.financesonline.com/p/chrome-enterprise/>

⁵⁶ Google Chrome Enterprise & Education FAQ, How is the Chrome Browser for the enterprise different than the consumer Chrome Browser?, URL: https://support.google.com/chrome/a/answer/188447?hl=en&ref_topic=4386908

⁵⁷ Google, G Suite Admin Help, Overview: Manage devices with Google endpoint management, URL: <https://support.google.com/a/answer/1734200>

device, the Device Policy App. This requires end users to have access to the Google Play Store, which is an Additional Service.

As Google explains to admins in public guidance:

*"If you chose to turn off Google Play for end users in your domain, expect to see the following: (...)You will be unable to manage your business's new mobile devices from the Google Admin console because the Device Policy app must be downloaded from Google Play."*⁵⁸

In reply to this DPIA, Google noted that end users are free not to use Android phones, as they can also buy an iPhone and download the Device Policy App from the Apple app store.

1.4.4 *Technical Support Services and Support Data*

Google provides Technical Support Services to G Suite Enterprise customers (Technical Support Services).⁵⁹ The actual data processing through a support request has not been tested for this DPIA, in order not to burden Google with a fake support request. This DPIA does assess the risks for data subjects resulting from the use of these services based on the contractual guarantees.

Google refers to the data it obtains in connection with the Technical Support Services as Support Data. In the Technical Support Services Guidelines (TSS Guidelines), Google defines Support Data as "account details and the information that Customer provides to Google for the purpose of obtaining TSS under these Guidelines, including requests for support and the details provided to Google about the specific support issue."⁶⁰

According to the TSS Guidelines, Google collects and processes Support Data for the purpose of providing the support services described in these Guidelines and maintaining the Services.⁶¹ At the time of the completion of this report, Google did not provide additional information. On 12 November 2020 Google published a Google Cloud Privacy Notice with a list of purposes.⁶²

Google explained in response to this DPIA it has strict rules for access to Customer Data. With Google's product Access Transparency customers can view the reason for each access in some Core Services, including references to specific support tickets where relevant.⁶³ Google also explained: "Google remains a data processor in respect of Customer Personal Data accessed by Support agents in order to provide support."⁶⁴

Google explicitly warns administrators that the (consumer) Privacy Policy applies when submitting troubleshooting information to Support. See Figure 9 below. The boundaries between Support Data and Customer Personal Data in Support Requests are not clear to customers. See Section 5.3.5.

⁵⁸ Google, G Suite Admin Help, Turn Google Play on or off for end users, under 'Next steps', URL: <https://support.google.com/a/answer/7080240?hl=en>

⁵⁹ As well as services identified as 'Other Services' in the G Suite Services Summary and services described in the Complementary Product Services provided under a separate agreement. These services are out of scope of this DPIA.

⁶⁰ G Suite Technical Support Services Guidelines, Section 7.13, URL: <https://gsuite.google.com/terms/tssq.html>

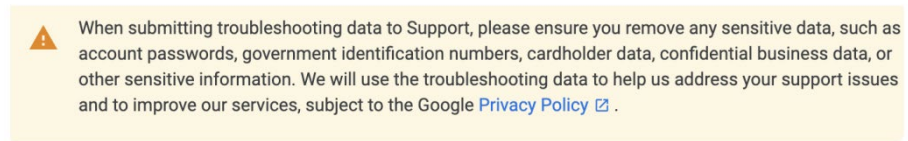
⁶¹ Idem, Section 6.4.

⁶² Google, Google Cloud Privacy Notice, 7 December 2020, URL: <https://cloud.google.com/terms/cloud-privacy-notice>

⁶³ Google Access Transparency Log, URL: <https://cloud.google.com/logging/docs/audit/access-transparency-overview>

⁶⁴ From responses provided by representatives of Google to SLM Microsoft Rijk during the course of the DPIA

Figure 9: Google warning to administrators when they ask for Support



1.4.5

Other related services that may download or analyse content

The *Feedback* module offers end users the possibility to give feedback to Google about the quality of information on its webpages, or report problems. In this 'Feedback' module, the end user is invited by default to send a screenshot to Google, but he/she can also send free text. In the text box, Google mentions that it can use the data to improve the services, and refers to its (consumer) Privacy Policy. Google confirmed in reply to this DPIA that Feedback is "a voluntary feature and data is processed according to the Google Privacy Policy."⁶⁵ This means that Google may process data submitted by employees for the 33 purposes of its (consumer) Privacy Policy (see Section 4.2 of this report).

Google explained that there is a difference between the Feedback module on the one hand, and the Features *Spelling and Grammar*, *Translate* and *Explore* on the other hand. Google explained that Feedback module is an optional service, that falls under the (consumer) Privacy Policy, while the three Features are part of the Core Services.⁶⁶

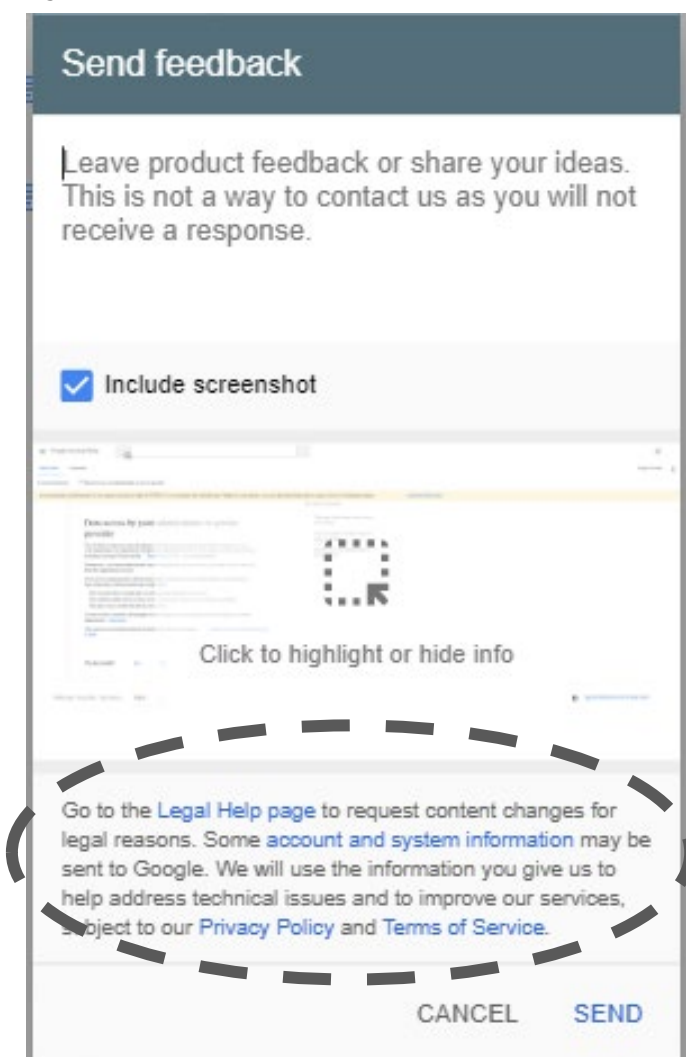
Google does not publish documentation about such Other related services. In this DPIA, the existence of the Feedback module was observed, but it is unknown how many other services Google offers in connection with the Core Services that are not part of the Core Services.

Another example of this category of Other related services is the *Enhanced Spellcheck* in the Chrome browser, which Google qualifies as a consumer product.

⁶⁵ Google reply to part A of the DPIA.

⁶⁶ Google feedback on part A of the DPIA.

Figure 10: Feedback



1.5 The enrolment framework for G Suite Enterprise

Google generally offers G Suite Enterprise as an online enrollment, that can be procured on its website. However, large customers such as the Dutch government may enter into a specific offline agreement called the Cloud Master Agreement.

In Clause 2.1 of the G Suite DPA Google explains that there are different types of enrollment agreements: "**G Suite Agreement**" means a G Suite Agreement; a G Suite for Education Agreement; a Google Cloud Master Agreement with G Suite Services Schedule; or any other agreement under which Google agrees to provide any services described in the G Suite Services Summary to Customer."⁶⁷

This report uses the most recently available public versions of the relevant contractual documents.

⁶⁷ Data Processing Amendment to G Suite and/or Complementary Product Agreement (Version 2.2), Section 2.1 Definitions, URL: https://gsuite.google.com/terms/dpa_terms.html, hereinafter: G Suite DPA.

1.5.1 *Relevant data protection terms and conditions*

The following documents may contain data protection terms for G Suite Enterprise:

- G Suite DPA
- G Suite EU Model Contract Clauses (separate agreement entered by Google LLC with the customer)
- G Suite Service Specific Terms⁶⁸
- G Suite [Core] Services Summary⁶⁹
- Google Additional Product Terms⁷⁰
- G Suite Acceptable Use Policy⁷¹
- G Suite Technical Support Services Guidelines (TSS)⁷²
- +
- Google Privacy Policy for end users⁷³
- Google Terms of Service for end users⁷⁴
- Separate Terms⁷⁵ and Privacy Notice for Chrome browser and OS⁷⁶

Note: after completion of this report in July 2020, Google published new documents and negotiated a privacy amendment with the Dutch government. These improvements are described in the new assessment of the risks added to the summary and conclusion of this report in January 2021.

1.5.2 *Google Account*

The G Suite DPA only applies to the Customer Data in the Core Services.⁷⁷

The G Suite DPA does not apply to the processing in connection with a Google Account (though Google has explained it does apply the G Suite DPA when the Account is used in conjunction with a Core Service), or to the use of the Additional Services, such as YouTube, Maps and Search.

Google explains: "*These products [Additional Services] are not part of the G Suite offering and are not covered by the G Suite DPA.*"⁷⁸

Google explained to the researchers that there is a hard distinction between the Core G Suite Enterprise services and the many consumer services Google offers globally.⁷⁹

⁶⁸ G Suite Service Specific Terms, URL: <https://gsuite.google.com/terms/service-terms/>

⁶⁹ G Suite Services Summary, URL: https://gsuite.google.com/terms/user_features.html

⁷⁰ Google Cloud Additional Product Terms, URL: https://gsuite.google.com/intl/en/terms/additional_services.html

⁷¹ Google G Suite Acceptable Use Policy, URL: https://gsuite.google.com/terms/use_policy.html

⁷² Google, G Suite Technical Support Services Guidelines, URL: <https://gsuite.google.com/terms/tssg.html>

⁷³ Google Privacy Policy. The version used for this report was last updated 31 March 2020, available at <https://policies.google.com/privacy?hl=en#intro>. URL last visited on 17 June 2020).

⁷⁴ Google (consumer) Terms and Services. The version used for this report was last updated on 31 March 2020, available at <https://policies.google.com/terms> (URL last visited 17 June 2020).

⁷⁵ Google, Google Chrome and Chrome OS Additional Terms of Service, URL: <https://www.google.com/chrome/terms/?hl=en>

⁷⁶ Google Chrome Privacy Notice, Last modified: May 20, 2020, URL: <https://www.google.com/chrome/privacy/?hl=en>

⁷⁷ As well as services identified as 'Other Services' in the G Suite Services Summary and services described in the Complementary Product Services provided under a separate agreement. These services are out of scope of this DPIA.

⁷⁸ Google Workspace Data Protection Implementation Guide, December 2020, p. 5, URL: https://services.google.com/fh/files/misc/google_workspace_data_protection_guide_en_dec2020.pdf

⁷⁹ [CONFIDENTIAL]

In the new Google Terms of Service (effective 31 March 2020), Google explains that these consumer terms apply to the data processing as a result of the use of the Additional Services.⁸⁰ All end users with a Google Account must accept these (consumer) Terms of Service, regardless if they create the account as a consumer or as an employee in the enterprise environment. Google explains that this is because their G Suite credentials may be used to sign into and use consumer services if their IT administrator does not restrict such use.⁸¹

Google explains to administrators that they can disable access to the Additional Services if they cannot bind their end users (government employees) to these terms.

"If Customer does not wish to enable any Additional Products, or if you are acting on behalf of Customer but do not have the requisite authority to bind Customer to these Additional Product Terms, please disable such Additional Products via the functionality of the Services."⁸²

2. Personal data and data subjects

The Dutch government DPIA model requires that this section provides a list of the kinds of personal data that will be processed via the Diagnostic Data, and per category of data subjects, what kind of personal data will be processed by the product or service for which the DPIA is conducted. Since this is an umbrella DPIA, this report can only provide an indication of the categories of personal data and data subjects that may be involved in the data processing. As the categories of personal data and data subjects in Customer Data and Support Data are dependent on the data that the customer and its end users provide to Google, this Section focusses on the data that is collected by Google through the use of the services (Diagnostic Data).

The section provides arguments why the Diagnostic Data processed by Google about the individual use of the G Suite Core and the tested Additional Services, the Google Account and the telemetry data from the apps and the Chrome browser are personal data. Section 2.3 contains the analysis of outgoing traffic.

2.1 Definitions of different types of personal data

2.1.1 Definitions GDPR

Article 4(1) of the GDPR provides the following definition of personal data: *'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.'*

The concept of processing is defined in Article 4(2) of the GDPR:

"'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration,

⁸⁰ Google, updated Terms of Service 31 March 2020: "We added a link to a page of service-specific additional terms that make it easier to find all the terms of use that apply to a particular service."

⁸¹ Google reply to part A of the DPIA.

⁸² Ibid.

retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."

Article 4(5) of the GDPR contains a definition of pseudonymisation:

"the processing of personal data in such a way that the personal data can no longer be linked to a specific data subject without the use of additional data, provided that these additional data are stored separately, and that technical and organisational measures are taken to ensure that the personal data are not linked to an identified or identifiable natural person."

The GDPR clearly explains that pseudonymised data are still personal data, to which the GDPR applies. Recital 26 explains:

"Pseudonymised personal data that can be linked to a natural person through the use of additional data should be regarded as data relating to an identifiable natural person. In order to determine whether a natural person is identifiable, account must be taken of all means that can reasonably be expected to be used by the controller or by another person to directly or indirectly identify the natural person, for example selection techniques. In determining whether any means can reasonably be expected to be used to identify the natural person, account shall be taken of all objective factors, such as the cost and time of identification, taking into account available technology at the time of processing and technological developments."

2.1.2 *Definitions Google's (consumer) Privacy Policy*

Google obtains personal data in different ways. Directly from government employees when they create a Google Account and use the services to upload Customer Data, and indirectly, in system generated logfiles about the interactions with its cloud services, as well as through telemetry files sent from devices to Google.

In its (consumer) Privacy Policy Google uses the term 'personal information', rather than the term personal data. Google defines 'personal information' as follows:

"This is information that you provide to us which personally identifies you, such as your name, email address, or billing information, or other data that can be reasonably linked to such information by Google, such as information we associate with your Google Account."⁸³

Although the definition of 'personal information' in the General Privacy Statement does not directly oppose what is defined as 'personal data' under the GDPR, it is unclear whether all data that would qualify as personal data under the GDPR also fall in the scope of the definition of 'personal information' used by Google.

2.1.3 *Definitions G Suite DPA*

In the G Suite DPA, Google uses the term 'personal data' with reference to the GDPR definition. However, the G Suite , DPA does not apply to all personal data. In the G Suite DPA, Google's role as a data processor is limited to Customer Data, i.e., data submitted, stored, sent or received via the Services by the customer or end users.

The G Suite DPA therefore only applies to the processing of personal data in Customer Data. Google defines such data as 'Customer Personal Data' in the G Suite DPA.

⁸³ Pop-up in the google Privacy Policy.

While "Customer Data" includes information that end users consciously upload to G Suite Services, such as a document authored outside of G Suite Services and then saved to Drive, "Customer Data" also includes:

- information the end user generates directly with G Suite, such as a message typed in Hangouts Chat;
- information generated by G Suite at the customer's request, such as the output of numerical calculations computed in Google Sheets; and
- information G Suite receives on behalf of the customer, such as an email sent to a customer's end user in Gmail by a third party outside of the customer's domain.⁸⁴

Diagnostic Data

Diagnostic Data are not part of the G Suite DPA, as it is limited to Customer Data. Customers may not be aware of this exclusion, as Google does not publish documentation about this at the time of completion of this DPIA.

During this DPIA, Google explained that it generally processes Diagnostic Data under its (consumer) Privacy Policy, and not under the G Suite DPA:

*"The laws, terms and conditions that would apply to the processing of Diagnostic Data, (...) depend on a variety of factors that cannot be ascertained conclusively without a clarification of the exact data that is being referred to. However in as far as such data includes personal data processed by Google, **Google's Privacy Policy is likely to apply to such processing** and the GDPR may apply to such processing under the conditions of Art. 2 and 3 GDPR."*⁸⁵

In its (consumer) Privacy Policy, Google does not use the term Diagnostic Data, but refers to the collection of 'information'.

"The information we collect includes unique identifiers, browser type and settings, device type and settings, operating system, mobile network information including carrier name and phone number, and application version number. We also collect information about the interaction of your apps, browsers, and devices with our services, including IP address, crash reports, system activity, and the date, time, and referrer URL of your request.

*We collect this information when a Google service on your device contacts our servers — for example, when you install an app from the Play Store or when a service checks for automatic updates. If you're using an Android device with Google apps, your device periodically contacts Google servers to provide information about your device and connection to our services. This information includes things like your device type, carrier name, crash reports, and which apps you've installed."*⁸⁶

It is unclear from the (consumer) Privacy Policy whether Google qualifies all or part of such 'information' (i.e. Diagnostic Data) as personal data. Google's answer to Privacy Company suggests that Google does not exclude that personal data may be included in Diagnostic Data:

*"However in as far as [Diagnostic Data] includes personal data processed by Google, Google's Privacy Policy is likely to apply to such processing and the GDPR may apply to such processing under the conditions of Art. 2 and 3 GDPR."*⁸⁷

⁸⁴ From responses provided by representatives of Google to SLM Microsoft Rijk during the course of this DPIA.

⁸⁵ Idem.

⁸⁶ Google general Privacy Policy.

⁸⁷ Idem.

Google Account

As explained in Section 1.4.2, end users have to create a Google Account in order to use the G Suite Enterprise services. In principle, Google processes data relating to a Google Account (as a data controller) under its (consumer) Privacy Policy. However, Google explained that when a Google Account is used to access a Core Service, the processing is subject to the G Suite DPA, rather than the (consumer) Privacy Policy:

"We consider Google Accounts to primarily serve as engineering infrastructure by which an end user authenticates and gains access to whatever services the end user is allowed to access by virtue of its relationship with Google. Google Account is processed in the same way as Core Service data when its functionality is used in conjunction with Core Services (to which the G Suite DPA, rather than the Google Privacy Policy would apply)."⁸⁸

Support Data

As described in Section 1.4.4, G Suite includes technical support services relating to the Core Services (Technical Support Services).⁸⁹ Google refers to the data it obtains in connection with the Technical Support Services as Support Data. In the Technical Support Services Guidelines (TSS Guidelines), Google defines Support Data as 'account details and the information that Customer provides to Google for the purpose of obtaining TSS under these Guidelines, including requests for support and the details provided to Google about the specific support issue.'

According to the TSS Guidelines, Google collects and processes Support Data for the purpose of providing the support services described in these Guidelines and maintaining the Services.⁹⁰ Google does not provide additional information.

2.2 Diagnostic Data

As explained in Section 1.2, Google collects Diagnostic Data in multiple ways. Sections 2.2 to 2.4 discuss how Privacy Company obtained access to Diagnostic Data in the context of this DPIA and contains an overview of the content of such Diagnostic Data.

Though Google provides extensive documentation about the existence and contents of the logs that it makes available for administrators, there is very little public documentation about other Diagnostic Data Google collects, such as telemetry data, or other data Google collects on its servers about the use of G Suite Enterprise applications.

2.2.1 Audit logs and visual reports

Google stores Diagnostic Data about the use of its cloud services in log files. Google makes some of these logs available for admins in so-called audit logs. There is no public documentation what logs Google collects in system generated logs, and what data it makes available for admins.

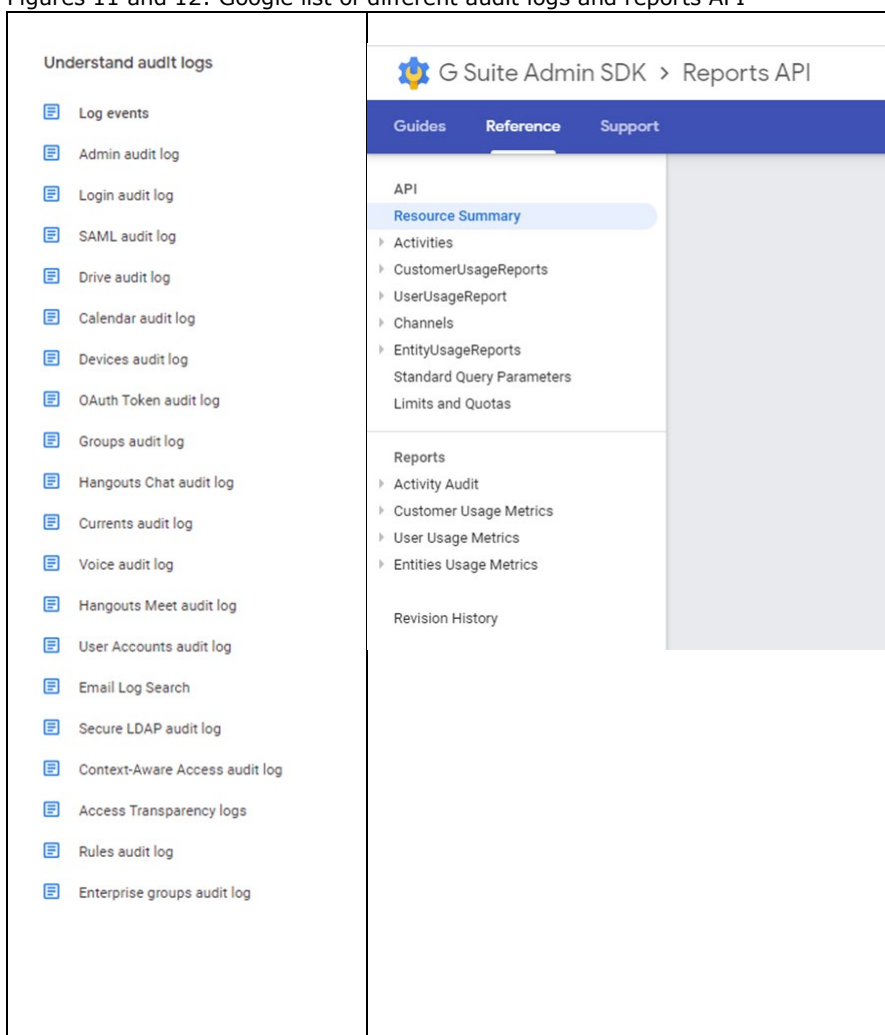
The audit logs provide some information about the Diagnostic Data Google collects. Another source of information used for this report, is traffic interception from the installed apps. This will be discussed below, in Section 2.3.

⁸⁸ Google reply to part A of the DPIA.

⁸⁹ As well as services identified as 'Other Services' in the G Suite Services Summary and services described in the Complementary Product Services provided under a separate agreement. These services are out of scope of this DPIA.

⁹⁰ Clause 6.4 G Suite Technical Support Services Guidelines.

Figures 11 and 12: Google list of different audit logs and reports API



Admins can access 19 kinds of audit logs through the Google Admin Console.⁹¹ These are: Admin, Login, SAML, LDAP, Drive, Calendar, Context-Aware Access, Devices, Password Vault, Token, Groups, Hangouts Chat, Google+, Voice, Hangouts Meet, User Accounts, Access Transparency and Rules.⁹² Additionally, admins can use a separate Email Log Search. For this DPIA, 13 logs about services in scope of this DPIA were analysed.

Google also makes these logs available through its API so that administrators can obtain automated, almost realtime access to end user activities.⁹³

Google additionally provides four types of visual reports:⁹⁴

1. Activity log files (activities of end users and administrators)
2. Customer Usage Metrics (aggregated properties and statistics for all end users, across an entire Enterprise domain)

⁹¹ Google, understand audit logs, URL:

https://support.google.com/a/answer/6098211?hl=en&ref_topic=9027054

⁹² The following 5 logs were empty, because the functionality was not tested: SAML, LSDAP, Context-Aware Access, Voice and Password Vault.

⁹³ <https://developers.google.com/admin-sdk/reports/v1/guides/manage-audit-drive>

⁹⁴ Google API Reference, URL: <https://developers.google.com/admin-sdk/reports/v1/reference/>

3. User Usage Metrics (individual Diagnostic Data. *“The end user usage report returns G Suite service usage information for a particular end user in your domain. These reports can be customized and filtered for specific usage information. The default and maximum time period for each report is the last 450 days”*⁹⁵; and
4. Entities Usage Metrics (only about the use of Google+)

The logs and reports show that Google logs personal data at a granular level about individual end user actions in three different categories: application usage (such as Gmail or Docs), file access (any activity related to the opening, changing, saving and sharing of files) and access to third party services using the Google credentials (Cloud Identity).

The **Drive Audit log** file contains file and path names, in combination with the email address of the end user.

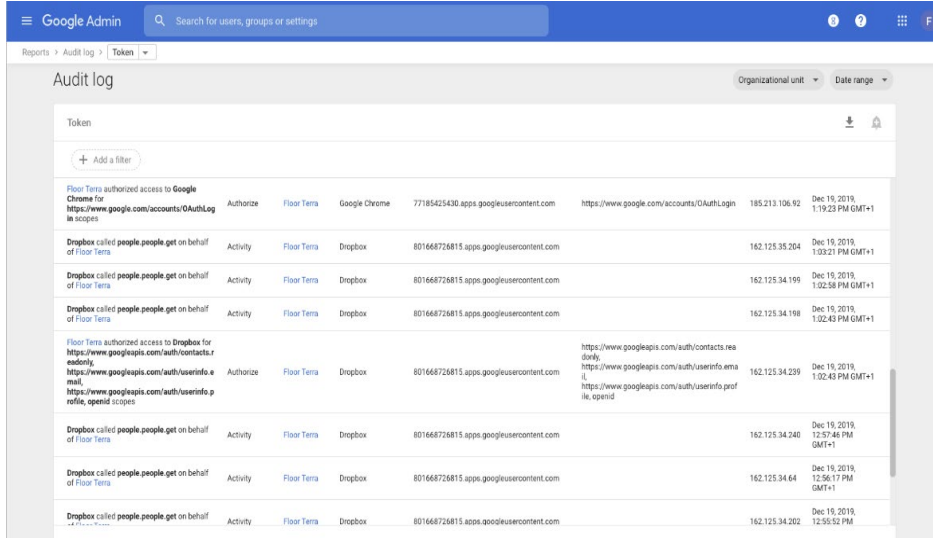
Table 7: Drive Audit log

Item name	Name of document with URL (path name)
Event description	Username and executed action, such as 'edited' 'viewed' or 'downloaded'
User	Username and link to the account of the end user who executed the actions.
Date	Timestamp with time zone
Event name	For example: view, download or edit
Item ID	Unique identifier for the document
Item type	For example: Google Docs or Slides
Owner	Email address of the owner of the document
(Prior) visibility	Whether a document is visible or accessible.
IP	Full IP address

The **Token audit log** contains a log of authentication tokens that applications and websites use to access Google Account. In the tests executed for this DPIA, authentications tokens to log in to Chrome, Dropbox, iOS and Android were logged. For each event the type (creation, use or revocation), end user account, the application or website, the end user’s IP address and timestamp were logged. Thus Google collects information on the use of websites and apps by an end user with a corporate G Suite authentication token.

⁹⁵ Google Report API: Users Usage Report, URL: <https://developers.google.com/admin-sdk/reports/v1/guides/manage-usage-end-users>

Figure 13: Example of Token audit log



Many websites and apps accept easy sign-in with a Google Account. This is convenient for end users, because they will not have to remember separate credentials for each website or app., It is reasonable to expect that end users will frequently use their Cloud Identity Google Account for single sign-on services. In the G Suite Enterprise environment, this has as a side effect that the Token audit log allows administrators to view on what websites and apps end users have logged with their Google account.

Google notes:

*"G Suite audit and reporting help administrators track important activities. Log-in activity for third-party apps is included so administrators have a complete picture in one place."*⁹⁶

A third example of logging is shown in the reports that provide an overview of activities of one end user in one application, for example the use of Gmail.⁹⁷

The Gmail usage reports provide aggregated information about one specific individual's email behaviour, such as the total number of emails sent and received in the last 450 days, and the last time they accessed their mail through webmail, pop or imap.

Table 8 Overview of individual end user actions in Gmail

is_gmail_enabled	boolean	If true, the end user's Gmail service is enabled
num_emails_exchanged	integer	The total number of emails exchanged. This is the total of num_emails_sent plus num_emails_received
num_emails_received	integer	The number of emails received by the end user

⁹⁶ Google, Google Identity Services for work, URL: <https://storage.googleapis.com/qfw-touched-accounts-pdfs/google-identity-takeaway.pdf>

⁹⁷ Google Gmail Parameters, URL: <https://developers.google.com/admin-sdk/reports/v1/appendix/usage/user/gmail>

num_emails_sent	integer	The number of emails sent by the end user
num_spam_emails_received	integer	The number of emails received by the end user's marked as spam mail
timestamp_last_access	integer	Last access timestamp
timestamp_last_imap	integer	Last imap access timestamp
timestamp_last_interaction	integer	Last interactive access timestamp
timestamp_last_pop	integer	Last pop access timestamp
timestamp_last_webmail	integer	Last web access timestamp

Google also creates aggregated statistics about Gmail usage in the Customer Usage Metrics.⁹⁸

These statistics contain much more information about email behaviour, such as the number of encrypted inbound and outbound mails, and the number of inbound spam emails. Such information can be useful for administrators if they would want to change their security policy to for example ban unencrypted mails. These logs can also inform an administrator if a particular end user suddenly receives a lot of spam. Without these user specific reports, it would require more effort to retrieve this information from the general Email logs.⁹⁹

Figure 14: G Suite Reports API: export Gmail actions

The screenshot shows the 'G Suite Admin SDK > Reports API' page. On the left is a navigation sidebar with categories like 'API', 'Reports', and 'Revision History'. The 'Reports' section is expanded to show 'Customer Usage Metrics', with 'Gmail' selected. The main content area displays a list of metrics:

num_7day_imap_users	integer	The number of users who accessed IMAP in the past 7 days from the date of this report.
num_7day_pop_users	integer	The number of users who accessed POP in the past 7 days from the date of this report.
num_7day_webmail_users	integer	The number of users who accessed their web Gmail accounts in the past 7 days from the date of this report.
num_emails_exchanged	integer	The total number of emails exchanged. This is the total of num_emails_sent plus num_emails_received.
num_emails_received	integer	The total influx of emails received on the date of this report.
num_emails_sent	integer	The number of emails sent on the date of this report.
num_inbound_delivered_emails	integer	The number of delivered inbound emails on the date of this report, rerouted emails are not included in this report.
num_inbound_encrypted_emails	integer	The number of encrypted inbound emails on the date of this report.
num_inbound_non_spam_emails	integer	The number of inbound non-spam emails on the date of this report.
num_inbound_rejected_emails	integer	The number of rejected inbound emails on the date of this report, rerouted emails are not included in this report.
num_inbound_rerouted_emails	integer	The number of rerouted inbound emails on the date of this report.
num_inbound_spam_emails	integer	The number of inbound spam emails on the date of this report.
num_inbound_unencrypted_emails	integer	The number of unencrypted inbound emails on the date of this report.
num_outbound_delivered_emails	integer	The number of delivered outbound emails on the date of this report. Rerouted emails are not included in this report.
num_outbound_encrypted_emails	integer	The number of encrypted outbound emails on the date of this report.
num_outbound_rejected_emails	integer	The number of rejected outbound emails on the date of this report. Rerouted emails are not included in this report.
num_outbound_rerouted_emails	integer	The number of rerouted outbound emails on the date of this report.
num_outbound_unencrypted_emails	integer	The number of unencrypted outbound emails on the date of this report.

⁹⁸ Google G Suite Admin SDK, Reports API, Gmail Parameters, URL: <https://developers.google.com/admin-sdk/reports/v1/appendix/usage/customer/gmail>

⁹⁹ See Google, Email Log Search, URL: https://support.google.com/a/topic/2618873?hl=en&ref_topic=9027054

2.3 Outgoing traffic analysis

As detailed in [Appendix 1](#), tests were executed on the webbased applications on Windows 10 and macOS platforms with the Chrome browser, as well as in the installed iOS and Android apps (the latter installed on a Chromebook).

While the scripted scenarios were executed, the outgoing traffic was intercepted. Interception of the traffic generated by the iOS apps was not possible with the regular MiTM proxy procedure, because the traffic is protected against interception with certificate pinning. Instead, the traffic was intercepted with Wireshark. This results in a higher level of uncertainty about the contents of the captured network traffic from the iOS apps. It was not technically possible to (separately) capture or analyse the telemetry traffic. Nonetheless, the traffic analysis provides insights in the processing of Diagnostic Data by Google.

In the test set-up, all default settings were left unchanged. Therefore, the test accounts had access to all Additional Services.

The tests resulted in a high volume of traffic to third parties and to external advertising domains. The observed data streams to third parties were not caused by the Core Services themselves, but by the test users:

- to test the Cloud Identity Services, Dropbox was authorised for single sign-on; and
- to test Google+, the scenarios included visits to two Dutch news websites that place a lot of advertising cookies.

Other findings are:

- Google DoubleClick collects data when a non-authenticated end user visits a login page for the Core Services. Google has explained the presence of the DoubleClick cookie is legitimate, because these cookies are used *“to determine eligibility for ads personalization. This cookie communicates to DoubleClick whether a specific end user is eligible for personalized ads because of their account status or ads personalization preferences.”*¹⁰⁰
- In another case, a DoubleClick cookie was encountered through an embedded Youtube iframe inside the Drive webpage.¹⁰¹ Google was able to reproduce the event described by the researchers and determined that this DoubleClick cookie was set by mistake and not intended product behaviour. Google explained that Drive was accidentally showing a welcome video using the YouTube player, without suppressing Ads integration.¹⁰² Privacy Company has verified that Google has fixed this bug.
- The Additional Service Google Maps is integrated with several Core Services. In Calendar traffic to Google Maps takes place when working with Calendar items that contain a location. Traffic to Google Maps was also observed from Google+ posts with a location tag and a page in Sites with an embedded map. The geoservice integration of Maps in Calendar means all addresses entered in the Calendar for meetings are automatically checked and corrected with information from Google Maps. In reply to this DPIA, Google explained that the traffic to Maps was not traffic to an Additional Service, but an embedded processing within the Core Services. As described in Section 1.4.3 Google explained that such traffic from the Calendar, Google+ and Sites Core Services to Google Maps is a *Feature* of the Core Services, and the personal data are *anonymised* before the traffic is

¹⁰⁰ Google response 5 June 2020.

¹⁰¹ https://drive.google.com/drive/my-drive_page.

¹⁰² Google response 5 June 2020.

As shown in [Figures 7 and 8](#), there are two types of spellcheckers available in the Chrome browser: a local *Basic Spellcheck* and a cloud-based *Enhanced Spellcheck*. The *Enhanced Spellcheck* is disabled by default. End users can individually enable the *Enhanced Spellcheck*. The use of the *Enhanced Spellcheck* cannot be centrally prohibited by administrators. As explained in Section 1.4.3, this functionality is only available if the customer purchases the separate product Chrome Enterprise. This product is covered by a separate Chrome Enterprise Upgrade agreement and a separate data processing agreement.¹⁰³

In this Chrome Enterprise Data Processing Agreement, Google defines the categories of data it collects via the managed Chrome browser as follows: “*Categories of Data, Data relating to individuals provided to Google via the Services, by (or at the direction of) Customer, its Affiliates, its Administrators, or End Users and may include the following categories of data: MAC address, network IP address, device location (if specified by Administrators), enrollment ID, Customer Hardware End Users’ login credentials, Customer Hardware End User’s, last activity time, Customer Hardware End User app installation, and other data.*”

Privacy Company verified that it is possible to centrally disable the *Enhanced Spellcheck* with Chrome Enterprise (See [Appendix 1](#)).

2.3.1

Other telemetry data

As explained in Section 1.2, telemetry data is a subset of Diagnostic Data. Google can collect these data from its Chrome OS, Chrome browser and from locally installed apps. It is clear from the analysis and responses from Google that Google collects more telemetry data than could be detected through the network traffic interception described in Section 2.3.

In reply to questions from Privacy Company, Google provided some information about the telemetry data it processes. Google asked Privacy Company not to include this information in the public DPIA report, as Google generally considers information about the existence and contents of telemetry data confidential.

Google’s claim that there is no public information about telemetry, is not entirely correct.¹⁰⁴ At the time of completion of this DPIA, Google did publish some references to its collection of telemetry data.

Google writes in its (consumer) Privacy Policy:

“If you’re using an Android device with Google apps, your device periodically contacts Google servers to provide information about your device and connection to our services. This information includes things like your device type, carrier name, crash reports, and which apps you’ve installed.”¹⁰⁵

Some more information can be found in (specialist) information for Android developers.

“Since Android version 9, Google collects telemetry data from the device. The Diagnostic Data include information about app usage, battery and process statistics

¹⁰³ Google Data Processing Amendment to Chrome Agreement (Version 1.1), Last modified: Feb 6, 2019, URL: https://www.google.com/chrome/terms/dpa_terms.html

¹⁰⁴ The existence of telemetry data is mentioned in a discussion forum about fairphone. “Unfortunately the google apps are not the only preinstalled components on the FP3 that have undocumented telemetry capabilities and regularly or sporadically talk home.” URL: <https://forum.fairphone.com/t/telemetry-spyware-list-of-privacy-threats-on-fp3-android-9/55179/8>

¹⁰⁵ Ibid.

and crashes. In previous versions of Android, the telemetry stack was limited and didn't capture the information needed to identify and resolve system reliability and device or app issues. This made identifying root causes of issues difficult, if not impossible. Android 9 includes the statsd telemetry feature, which solves this deficiency by collecting better data faster. statsd collects app usage, battery and process statistics, and crashes. The data is analyzed and used to improve products, hardware, and services.”¹⁰⁶

It follows from this explanation that Google processes telemetry data from Android devices, for the purpose of ‘improving’ products, hardware and services.

Google publishes a list of all available raw stats log events from the Android apps, also known as ‘atoms’. As shown in detail in Appendix 1 to this DPIA, these log events include

- the local IP addresses with which the device is connected to the internet and its MAC address,
- what apps are used and when,
- Bluetooth use including the hashed MAC addresses
- when biometric authentication is used
- occurrence (not contents) of crashes and WTF's (What a Terrible Failure).¹⁰⁷

In addition, Google provides some public documentation about the crash data it collects through *Google Chrome and other projects*.¹⁰⁸ With the help of Breakpad, Chrome OS and the Chrome browser send crash reports as a minidump file. “A minidump file contains: (...)”

- *Other information about the system on which the dump was collected: processor and operating system versions, the reason for the dump, **and so on.***¹⁰⁹

In the separate privacy notice for the Chrome OS and Chrome browser, Google provides some information about the contents of its server logs.

“These “server logs” typically include your web request, Internet Protocol address, browser type, browser language, the date and time of your request and one or more cookies that may uniquely identify your browser.”¹¹⁰

It was technically not possible to (separately) capture or analyse the traffic from the Chrome OS and the Chrome browser from telemetry traffic generated about the use of the Core Services applications. Google does not offer tools similar to, for example, the Data Viewing Tool provided by Microsoft for end users to see what telemetry data have been sent from its Core Services apps. Google does not provide tools for admins either to see the data sent to Google.

¹⁰⁶ Google, Android 9 Release Notes, URL: <https://source.android.com/setup/start/p-release-notes>. Google refers to more information at frameworks/base/cmds/statsd/.

¹⁰⁷ The Android Open Source Project, atoms.proto, URL: <https://android.googlesource.com/platform/frameworks/base/+/refs/heads/master/cmds/statsd/src/atoms.proto>

¹⁰⁸ Google Chromium, starting with Breakpad, URL: https://chromium.googlesource.com/breakpad/breakpad/+/master/docs/getting_started_with_breakpad.md

¹⁰⁹ Google Chromium, URL: <https://chromium.googlesource.com/chromiumos/overlays/chromiumos-overlay/+/master/chromeos-base/google-breakpad/google-breakpad-9999.ebuild>

¹¹⁰ Idem, Section *Server Log Privacy Information*.

Privacy Company has had lengthy discussions with Google about different options to inspect the contents of the telemetry data. Google allowed Privacy Company to view (not capture or document) an example of telemetry traffic collected by Google in a test account from an engineer during a meeting, but did not provide any documentation about the entire path of the data collection or show any results of specific actions requested by Privacy Company.

In reply to this DPIA, Google points to the export possibility in Vault. This functionality allows administrators to export emails (contents, headers and folders) from Gmail and documents from Drive. The exports from Drive contain the created and modified dates for each file, with document types and titles.¹¹¹ However, this export only provides a very limited view on the Diagnostic Data Google collects about every user activity in its Core Services on its servers. The export does not include any information about the type of device and unique identifiers collected by Google about the user in telemetry and website data, nor does this export provide information about the use of Features, and whether Google collects fragments of content of documents stored in Drive. Other information also misses, as defined in Article 14(2), subsections a to g of the GDPR.

Additionally, Google noted in its response that end users can view certain Diagnostic Data like Drive or Gmail search queries¹¹² and review Diagnostic Data through the Drive activity dashboards.¹¹³ However, the first option does not yield results if an end user has chosen privacy friendly settings. In that case, the user can no longer see the registration by Google of activities, but that doesn't mean Google has deleted the data.¹¹⁴ Google explains that the activity data are no longer used when a user deletes activity from the dashboard.¹¹⁵

The second option (Drive activity dashboards) only shows what other end users have viewed a file an end user has actively shared. This does not constitute detailed information about the collection of Diagnostic Data.

Because of the lack of transparency, Privacy Company cannot determine the contents of the telemetry data. The telemetry that Privacy Company was able to analyse, contained personal data and sensitive content from files (in the *Enhanced Spellcheck* in Chrome, and in telemetry data about app usage). It cannot be ruled out that some, or all telemetry data contain (1) personal data in the form of unique end user and device information (2) information about app usage with timestamps, and (3) in some cases (sensitive) content that Google obtained as a data processor for Customer Data.

2.4 Results access requests

Google explains in its G Suite DPA that it is the customer's responsibility to answer data subject access requests.

"...if Google's Cloud Data Protection Team receives a request from a data subject in relation to Customer Personal Data, and the request identifies Customer, Google will advise the data subject to submit their request to Customer. Customer will be responsible for responding to any such request including, where necessary, by using the functionality of the Services."¹¹⁶

¹¹¹ <https://support.google.com/vault/answer/6099459>

¹¹² <https://myactivity.google.com/> .

¹¹³ Google, View the activity on your Google Docs, Sheets & Slides, URL: <https://support.google.com/docs/answer/7378739>

¹¹⁴ Google, How Google helps you manage data with My Activity, URL: <https://support.google.com/accounts/answer/9784401> Google writes: "If you delete activity, it's no longer used to personalize your Google experience."

¹¹⁵ Idem.

¹¹⁶ Google G Suite DPA, Sections 9.2.1 and 9.2.2.

Where Google is a data processor, it should provide the data controller (i.e. the government organisations) with information necessary to comply with data subject access requests. As explained in Section 2.3, the access Google provides to the personal data it processes in the available audit logs does not provide a complete overview of all information about all personal data processed by Google. This means that Google, in its role as data processor, does not provide customers with sufficient information to adequately respond to data subject access requests.

As analysed in more detail in Section 5 of this report, Google considers itself to be an independent data controller for the processing of Diagnostic Data, data relating to the Google Account (except when used in conjunction with a Core Service), data relating to the Additional Services, to Feedback, and data relating to ChromeOS and the Chrome browser. Where Google is an independent data controller, data subject access requests must be filed with Google.

To obtain access to these personal data, two formal data subject access requests were sent to Google for the personal data relating to the two test accounts.

Google responded by email of 27 February 2020, referring the researchers to the administrator log files.

"Please contact your account administrator, who has access to tooling and functionality to respond directly to your request. Your account administrator can provide you with personal data associated with your account and detailed logs of what actions you have taken while using G Suite Core Services. This would include, for example, what files you have created, read, updated, deleted or shared in Drive, email sent and received.

Additionally, some of the information you seek is already available to you via the end user interfaces of the products you are using and a number of secure online tools we provide to all end users to access their data. Please see the table below which provides an overview of these tools."¹¹⁷

Google provided hyperlinks to five download tools for the end-user.

As listed in [Table 9](#) below, none of these self-service tools show all the personal data Google collects, such as unique identifiers and content data, through (1) use of the Google Account in the Core Services, Additional Services and Other related services such as Feedback and the *Enhanced Spellcheck* in the Chrome browser, (2) the cookies and similar technologies used, plus the information recorded in the webserver access logs with information about IP address, end user and device to keep track of use of services through websites and apps and (3) information collected by the Chrome browser and Chrome OS, including device information from the Chromebook with Android apps that had access to the Play Store.

¹¹⁷ Google email reply to data subject access requests for the test accounts, 27 February 2020.

Table 9: Google overview of self-service tools for end users

Resource	Google explanation
User data export ¹¹⁸	A tool which enables end users to export and download [content] data.
My Activity ¹¹⁹ and view your Google Dashboard ¹²⁰	Allows end users to see and actively manage their recent activity and to manage the data in their Google Account.
Drive Activity Dashboard ¹²¹	Administrators and end users can access personal information related to their Drive file activity through the Drive Activity Dashboard. G Suite administrators can control whether end users see each other's file activity on an Activity Dashboard. File activity includes the names of end users who have viewed Docs, Sheets, and Slides files and the time they viewed them. Users can control whether their file-viewing information is displayed in the Activity dashboard. For example, if an administrator turns an end user's view history On, that end user can still choose privacy settings to hide the file views from the Drive Activity dashboard.
Review how you share data with third-party apps and sites ¹²²	List of sites and apps with access to the end user's Google Account.
Google's use of cookies ¹²³	A description and list of the cookies Google uses

Google added:

*"We are a data processor of Customer Personal Data as defined in the G Suite DPA. Our goal is to protect the privacy and security of our end users and we do not want to provide data to the wrong person. As discussed, we do not provide information where we do not believe there is a secure means of after-the-fact offline re-identification of a data subject in the context of a Subject Access Request, for example in situations where two or more individuals may use a device. Mobile Device Management is a solution for admins to control user/device policies and access."*¹²⁴

If end users have chosen privacy friendly settings, they cannot see any activity data in their personal dashboard. As explained above, in Section 2.3.1, this does not mean Google deletes the data.

Google explains in its (consumer) Privacy Policy:

¹¹⁸ Google, Download your data, URL:

<https://support.google.com/accounts/answer/3024190?hl=en>

¹¹⁹ Google, My Google Activity, URL: <https://myactivity.google.com/myactivity>

¹²⁰ Google Dashboard, See and manage the data in your Google Account, URL:

<https://myaccount.google.com/dashboard?pli=1>

¹²¹ Google, View the activity on your Google Docs, Sheets & Slides, URL:

<https://support.google.com/docs/answer/7378739?co=GENIE.Platform%3DDesktop&hl=en>

¹²² Google, Apps with access to your account, URL:

<https://myaccount.google.com/permissions>

¹²³ Google, How Google uses cookies, URL:

<https://policies.google.com/technologies/cookies?hl=en>

¹²⁴ Google response 5 June 2020.

*"Activity you keep helps Google provide you with a more personalized experience, including faster searches, automatic recommendations, and a better YouTube homepage. **If you delete activity, it's no longer used to personalize your Google experience.** (...) For business or legal compliance purposes Google must retain certain types of data for an extended period of time."*

Google also explains that it does not provide certain personal data in reply to a data subject access request, because (i) it is impossible to reliably verify the identity of the data subject as that of the requester and (ii) in some cases such transparency would hurt Google's efforts to protect the security of its systems

Google continues with an explanation why Google does not provide certain personal data, because Google finds it impossible to reliably verify the identity of the data subject as that of the requester, or because such transparency would hurt Google's own efforts to protect the security of its systems.

Google writes:

"Please note that certain personal data is not included in our responses to data subject access requests. For example, data is not included to the extent we are unable to verify that the person making the request is the data subject to which it relates (Article 11(2) and Article 12(2) GDPR). This applies, for example, to data that is associated with unique identifiers (e.g. so-called cookie IDs) where we are unable to verify that they relate to the person making the request. Additionally, data is not included to the extent that providing a copy of such data would adversely affect the rights and freedoms of others (Article 15 (4) GDPR). This applies, for example, to data we are processing in the context of detecting threats to the security of our system, the disclosure of which could impact the ability of others to safely use the services."¹²⁵

The researchers have offered Google multiple ways to verify their identity and properties of the (test)devices used to perform the scenarios, including providing detailed device, access and cookie identifiers, access to the intercepted data and a physical or virtual visit to a location to prove their identity, if necessary with copies of their passports. Google has refused all these options.

In sum, sections 2.2 to 2.4 show that the Diagnostic Data from the Core Services are personal data. The review of the audit logs available for administrators shows they contain IP addresses, end user and account identifiers, and sometimes email addresses. The telemetry logs recorded in Android Atoms and through the Chrome browser contain IP addresses, hashed MAC address and app usage data, and sometimes sensitive content of files (collected through use of the *Enhanced Spellcheck*).

Google only provides limited access to some usage data collected (in its role as data processor) about the use of some Core Services and the Google Account. These Diagnostic Data are generally personal data, since these data are generated by (and protected by access credentials) the activities of individual end users (data subjects).

Google fails to provide access to Diagnostic Data about the use of the Features and Additional Services, including the Chrome OS and Chrome browser. Google acknowledges in its reply to the data subject access requests that some data, such as cookie identifiers, are personal data, but Google states it cannot reliably verify that the person making the data subject access request is the data subject that these

¹²⁵ Google response 5 June 2020.

data relate to. Google was not willing to let the researchers provide additional information enabling their identification.

2.5 Types of personal data and data subjects

As emphasized above, this DPIA cannot provide the required limitative overview of the different categories of personal data that will be processed in the context of G Suite Enterprise. However, this report aims to provide assistance to the government organisations about these categories, to help them decide about the actual installation and settings based on an inventory of the categories of personal data that are factually processed in their specific organisation.

As the categories of personal data and data subjects in Customer Data and Support Data are dependent on the data that the customer and its end users provide to Google, this section focusses on the data that are collected by Google through the use of the services (Diagnostic Data).

2.5.1 Categories of personal data

Generally speaking, end user can process all kinds of personal data with G Suite Enterprise. The different services can be used for many different purposes by many different organisations. Absent a comprehensive documentation and publicly available policy rules governing the types of data that can be stored by Google as Diagnostic Data, it is prudent to assume that the G Suite Diagnostic Data may include all categories of personal data. Some types of data require extra attention due to their sensitive nature.

Classified Information

Depending on the capacity in which Dutch government employees work, they may process confidential government information or state secrets (Classified Information). The Dutch government defines four classes of Classified Information, ranging from confidential within a department to top secret.¹²⁶

Classified Information is not a separate category of data in the GDPR or other legislation concerning personal data. However, information processed by the government that is qualified as Classified Information, regardless of whether it qualifies as personal data, must be protected by special safeguards. The processing of this information may also have a privacy impact if such information relates to a specific individual. If the personal data of a government employee, such as his G Suite email address at the domain of his employer, or unique device identifier, reveals that this person works with Classified Information, the impact on the private life of this employee may be higher than if that employee would only process 'regular' personal data. Unauthorised use of Classified Information could for example lead to a higher risk of being targeted for social engineering, spear phishing and/or blackmailing.

Google acknowledges that there may be spill-over from an employee's 'private' Google Account to his enterprise Google Account.

*"When you're signed in with more than 1 Google Account at the same time, ads may be based on ad settings for your default account. Your default account is usually the account you signed in with first."*¹²⁷

¹²⁶ Amongst others, the categories of classified information are defined in the Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie (VIR-BI).

¹²⁷ Google, Control the ads you see, URL: <https://support.google.com/ads/answer/2662856>

If government organisations use Drive or Gmail, they have to be aware that the information stored on Google's cloud servers may include Classified Information from and about government employees, including information which employees regularly access, send or receive such confidential data.

Personal data of a sensitive nature

Some personal data have to be processed with extra care, due to their sensitive nature. Examples of such sensitive data are financial data, traffic and location data. Both the contents of communication as well as the metadata (Diagnostic Data) about who communicates with whom, are of a similar sensitive nature. The contents of communication are specifically protected as a fundamental right, but metadata (Diagnostic Data) deserve a high level of protection as well. This will be explained in more detail in Section 16 of this report.

The sensitivity is related to the level of risk for the data subjects if the confidentiality of such data is breached. The effect of a breach of personal data of a sensitive nature may pose a greater risk for the data subject of being targeted by criminals (e.g. blackmail, identity theft, financial fraud). Government employees may also experience a chilling effect as a result of the monitoring of their behavioural data. The audit logs for example could be used by the employer to reconstruct a pattern of the hours worked with the different applications. Such monitoring could lead to a negative performance assessment, if not specifically excluded in an (internal) privacy policy for the processing of employee personal data.

It is likely that many government employees will process personal data of a sensitive nature by using G Suite Enterprise. For example, employees may process sensitive financial data in relation to subsidies. Employees from the High Councils of State and Advisory Commissions are tasked to process sensitive personal data from individual requests and complaints from the Dutch public.

Personal data of a sensitive nature can be included in snippets of content of files that are provided to Google as Customer Data (such as the line preceding and following a word) in the telemetry data, as shown in [Figure 15](#). However, such snippets may also be included in system generated event logs about the use of the Additional Services such as Google Groups, Classroom, Photos or as keywords in Google Alerts. Path and filenames are included, as shown in the Drive audit log, in Diagnostic Data about the opening or saving of files in Drive or headers of mails in Gmail.

Special categories of personal data

Special categories of personal data are strongly protected by the GDPR. According to Article 9 (1) GDPR, special categories of data consist of any:

“personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation”.

With special categories of data, the principle is one of prohibition: these data may in principle *not* be processed. However, the GDPR contains specific exceptions to this rule. Special categories of personal data may be processed for instance when the data subject has explicitly consented to the processing, or when data are made public by the data subject, or when processing is necessary for the data subject to exercise legal claims.¹²⁸

¹²⁸ These specific exceptions lifting the ban on the processing are listed in Article 9(2) under a, e and f of the GDPR.

If government organisations such as the police and the judiciary worked with G Suite Enterprise, there is a risk that the Diagnostic Data may contain information on crimes and convictions, if such data are included in the file or path names.

2.5.2

Categories of data subjects

Generally speaking, the different categories of data subjects that may be affected by the processing of personal data, can be distinguished in three groups, namely: employees, contact persons and miscellaneous other data subjects.

Employees

The government end users of the G Suite Enterprise services are employees, civil servants, contractors and (temporary) workers of a governmental organisation.

Their names and other personal information are processed in connection with the documents they create and store in an online storage usually carrying their (last) name, be it Google Docs, Google Sheets, Google Slides, Google Forms or another file format. Their names and other personal data are also part of the emails they send and receive with Gmail.

Apart from the information generated by the employees themselves, employees are also data subjects in information generated by others. For instance, employees in the cc or bcc field of an email.

Contact persons

Information processed with the G Suite applications is often shared internally and externally. Customer Data and Diagnostic Data may contain information about contact persons who are not employees of the relevant government organisation. Examples are employees of other government organisations and third-party vendors. Diagnostic Data may include the sender's name and email address, as well as the time when an email was sent or received.

Dutch citizens and other data subjects

Besides employees and contact persons, personal data of other subjects that are not directly in contact with the government organisation may also be processed through the government organisation's use of G Suite Enterprise service. Such personal data could also occur in snippets of content included in the Diagnostic Data generated by the use of the G Suite Enterprise service. Diagnostic Data could also include information about the communications pattern with people that do not work for the Dutch government such as lawyers and other advisors. Other examples involve people whose information is forwarded, but who are not directly in touch with a Ministry themselves, or people who apply for a job.

In sum, there are no limits to the categories of data subjects whose data may be processed in Customer Data and Diagnostic Data under normal use conditions by employees of the Dutch government.

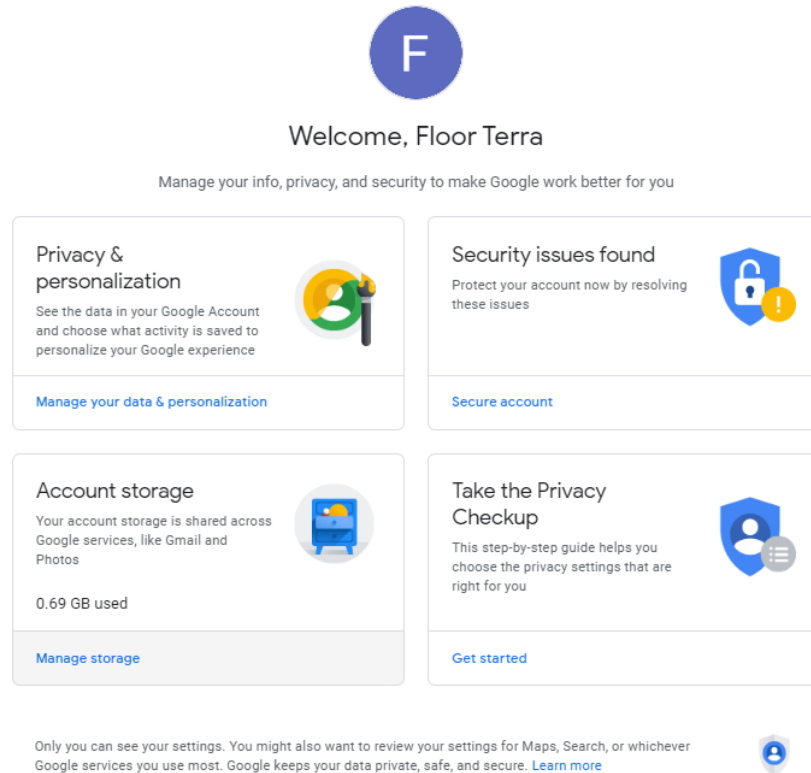
3. Data processing controls

This Section 3 discusses the available privacy controls that end users and administrators can use to influence the processing of Diagnostic Data, and the processing of personal data through the Additional Services and Related other services. This section also describes the *default* settings of such controls, and situations where admins do not have central privacy controls.

3.1 Privacy controls G Suite account for end users

As explained in Section 1.4.2, government employees must create a Google Account to use the G Suite services. New end users are shown a welcome message (see [Figure 6](#)) and are required to accept the Google Terms of Service and the Google Privacy Policy.

Figure 16: Google Account home screen, four controls for end users



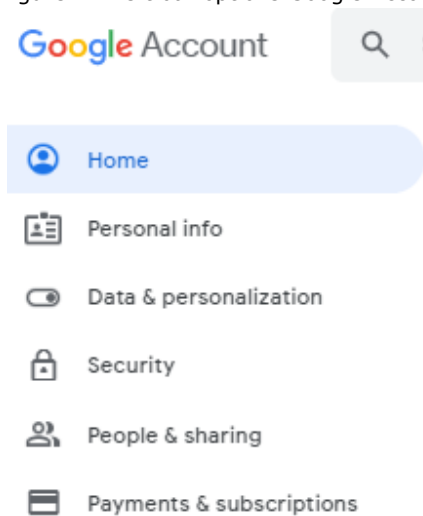
Once the Google Account is created, as shown in [Figure 16](#) above, end users of G Suite Enterprise are informed by Google about four topics on their account dashboard page accessible via myaccount.google.com

- Privacy & personalization
- Security issues found
- Account storage
- Take the Privacy Check-up

When selecting 'Privacy & personalization', Google shows nine different topics:

1. Take the Privacy Check-up
2. Activity controls (Web & App Activity, YouTube History and Ad personalization)
3. Ad personalization
4. Activity and timeline
5. Things you create and do
6. Account storage
7. Download or delete your data
8. General preferences for the web
9. Reservations

Figure 17: left bar options Google Account



If an end user clicks in the left bar of the main screen, and selects the topic 'Security', Google shows other privacy information, as shown in [Figure 17](#) to the left.

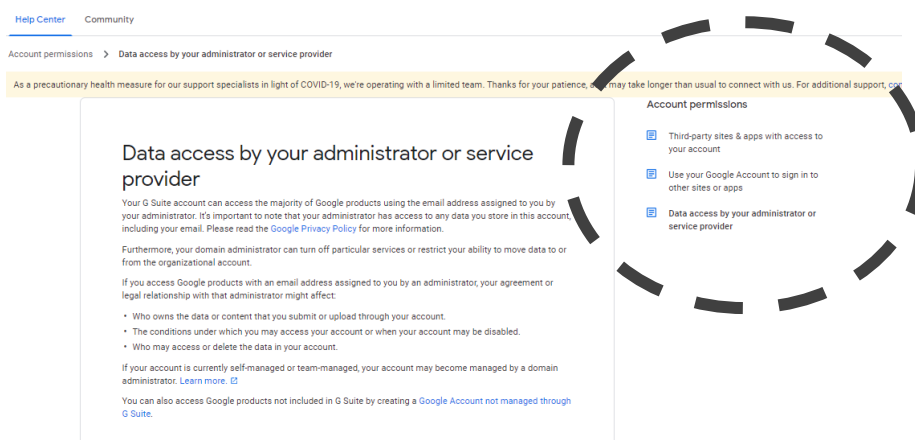
- Third party apps with account access
- Signing in to other sites with the Google Account

In its reply to this DPIA, Google mentions that one of the hyperlinks included in the Welcome Notice shown when creating the Google Account, refers to additional information in its help center about security and privacy options, such as creating a strong

password, controlling what others see about you across services, and turning off cookies.¹²⁹

Another relevant hyperlink in the Welcome Notice leads to a support article on Google Account permissions.¹³⁰

Figure 18: Information about Google Account permissions for end users



3.1.1

Access to Google Account information for third-party and Google sites & apps

Google explains that end users can allow some third-party apps limited, some or full access to information about their Google Account: access to basic profile information, access to some information such as contacts, photos or a YouTube playlist, or full access, to edit upload and create content in the Google Account.¹³¹ By default, no third-party apps have access.

¹²⁹ Google, Create a Google Account, URL:

<https://support.google.com/accounts/answer/27441>

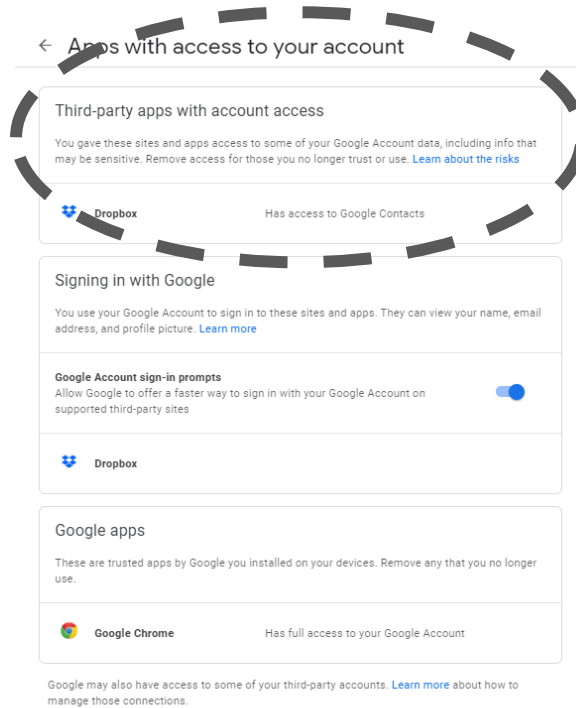
¹³⁰ Google, Data access by your administrator or service provider, URL:

<https://support.google.com/accounts/answer/181692?hl=en>

¹³¹ Google, Third-party sites & apps with access to your account, URL:

https://support.google.com/accounts/answer/3466521?hl=en&ref_topic=7188760

Figure 19: Viewing and controlling third party app access



The Chrome browser does have access to the Google Account by default, because Google considers this a trusted app, even though the Chrome browser is covered by separate product terms (see Section 1.5 of this report).¹³²

In the test scenarios, Dropbox was used to test the G Suite third party authentication tool Identity Management. The end-user can revoke access rights through the Security settings in the main control for the Google Account. See [Figure 19](#).

End users can remove access for the Chrome browser.

3.1.2

Using the Google Account to sign into other sites and apps

Government employees can use their Google Account as authentication to sign in with other sites and apps without having to create separate login credentials. This option is enabled by default. As shown above, in [Figure 19](#), end users can revoke such permissions to sign in with Google per individual app and site.

3.1.3

Administrator access to the data in Google Accounts

In the explanation about access to the Google Account by the administrators, as shown in [Figure 18](#), Google refers end users to its (consumer) Privacy Policy. Google explains: “Your G Suite account can access the majority of Google products using the email address assigned to you by your administrator. It’s important to note that your administrator has access to any data you store in this account, including your email. Please read the [Google Privacy Policy](#) for more information.”¹³³

In reply to this DPIA, Google added: “because G Suite end users may use their corporate credentials to use Additional Services in an authenticated state (Google Photos, for example), Google puts end users on notice that they may lose access to data processed by those Additional Services if their admin changes their configuration settings.”¹³⁴

Google explains in its Privacy Policy what data administrators can access:

¹³² In reply to this DPIA, Google refers to the possibilities in Chrome Enterprise for admins to determine privacy settings for end-users. However, this separate product is out of scope of this DPIA, as it is not included in the G Suite Enterprise contract.

¹³³ The hyperlinked words refer to a specific part of the general Google Privacy Policy, URL: <https://policies.google.com/privacy#infosharing>

¹³⁴ Google reply to part A of this DPIA.

"If you're a student or work for an organization that uses Google services (like G Suite), your domain administrator and resellers who manage your account will have access to your Google Account. They may be able to:

- *Access and retain information stored in your account, like your email*
- *View statistics regarding your account, like how many apps you install*
- *Change your account password*
- *Suspend or terminate your account access*
- *Receive your account information in order to satisfy applicable law, regulation, legal process, or enforceable governmental request*
- *Restrict your ability to delete or edit your information or your privacy settings."*¹³⁵

Google does not make more detailed information or examples available.

Google explains that end users may want to create a second unmanaged account to access services that are not included in G Suite Enterprise: *"You can also access Google products not included in G Suite by creating a Google Account not managed through G Suite."*¹³⁶ The underlined words contain a hyperlink referring to an explanation about how to create a new Google Account.¹³⁷ In this explanation, Google points employees to the possibility of bypassing possible restrictions set by administrators, for example, if the administrators prohibit the use of some or all of the Additional Services.

Google explained in reply to this DPIA that Enterprise customers may not prohibit an employee's personal use of Google services with his or her personal Google Account. Google objects against the conclusion that this can be read as an encouragement to bypass data protection measures.¹³⁸

3.1.4

Web & App Activity

In G Suite Enterprise Web & App Activity is disabled by default. Google explains what happens if end users decide to enable this control: *"Saves your activity on Google sites and apps, including associated info like location, to give you faster searches, better recommendations, and more personalized experiences in Maps, Search, and other Google services."*¹³⁹

¹³⁵ See footnote 122.

¹³⁶ Google, Data access by your administrator or service provider, URL: <https://support.google.com/accounts/answer/181692?hl=en>

¹³⁷ Google, Create a Google Account, URL: <https://support.google.com/accounts/answer/27441>

¹³⁸ Google reply to part A of this DPIA.

¹³⁹ Google, See & Control your Web & App Activity, URL: https://support.google.com/websearch/answer/54068?p=web_app_activity&hl=en.

Figure 20: Web & App Activity disabled by default

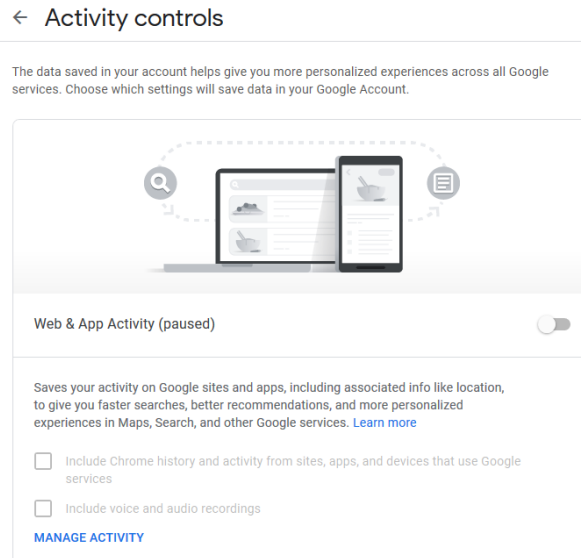
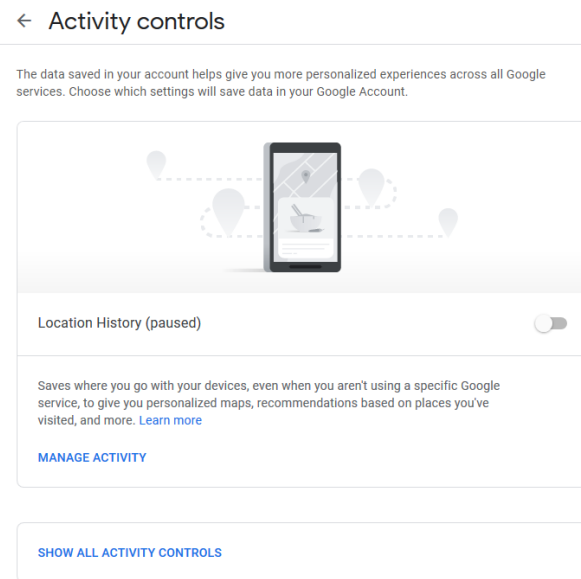


Figure 21: Location History disabled by default



3.1.5

Location History

Google has also disabled Location History by default, as shown in the tested G Suite Enterprise environment. Google explains that this function "Saves where you go with your devices, even when you aren't using a specific Google service, to give you personalized maps, recommendations based on places you've visited, and more."

Recently, Google processed the location data collected through Location History from end users who enabled the Location History, to proactively publish aggregated and anonymized statistics. Google explained it proactively wants to 'help public health officials combat COVID-19' with these data.¹⁴⁰

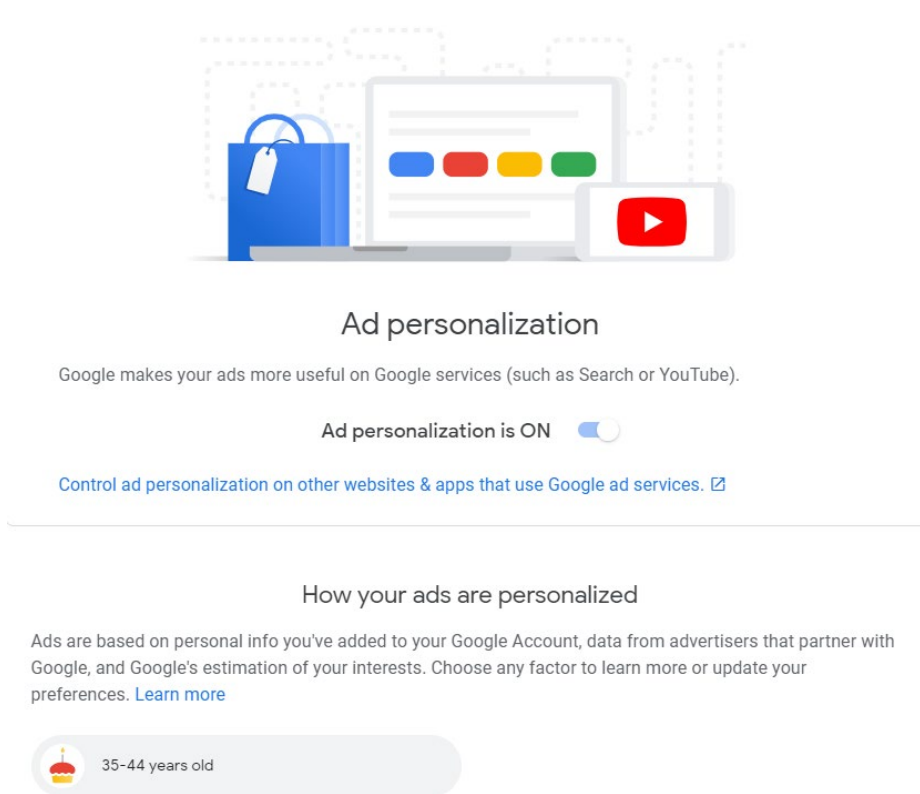
3.1.6

Ad personalization

¹⁴⁰ Google, Helping public health officials combat COVID-19, 3 April 2020, URL: <https://www.blog.google/technology/health/covid-19-community-mobility-reports>

When end users sign-in to their Google Account, and select 'Google Ad Settings', they can read how Google personalizes advertisements. By default, Ad personalization is turned On. See [Figure 22](#). Google clarified, in reply to this DPIA, that Ad personalization only applies to the use of consumer services (the 92 consumer services mentioned in [Table 6](#))

Figure 22: Google Ad Settings for Ad personalisation



In the test account, the personalization is based on the age group of the research account. Google has this information because end users are required to provide a date of birth when creating a Google Account.

Users can opt out from different interests, and synchronise these preferences across different devices. If they are signed in to multiple Google Accounts simultaneously, for example a Google Account relating to their employment and a Google Account they use for personal use, there is no separation of ads personalisation between these Google Accounts. Rather, ad personalisation is based on the default account for all Google Accounts that are logged into.

"When you're signed in with more than 1 Google Account at the same time, ads may be based on ad settings for your default account. Your default account is usually the account you signed in with first."¹⁴¹

This explains why G Suite Enterprise end users may see ads in their browser, when using their employment related Google Account, in spite of Google's promise that it will not show ads in the Core Services in the enterprise environment.

¹⁴¹ Google, Control the ads you see, URL: <https://support.google.com/ads/answer/2662856>

If an employee is signed in with his employment related Google Account, and uses (the consumer service) Google Search, Google treats the user as an anonymous visitor. Google only shows contextual ads, related to the search query, and does not ad specific interests to the work Google Account.

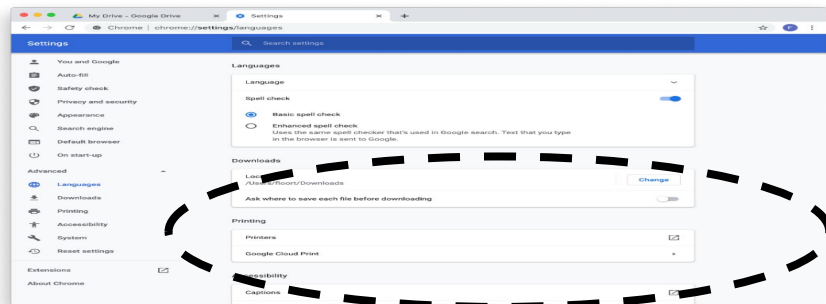
However, if the user has first logged in with his or her personal Google Account, while also logging-in with their Enterprise account, information about the contents of these work-related Searches can be added to the personal account as preferences to the consumer profile.¹⁴² Google does not provide a separate warning that advertising information may thus spill over from the work to the personal Google Account.

3.1.7 Chrome and Chrome OS

On the Chromebook and in the Chrome browser, end users can access different privacy and security settings controlling the data collection via the Chrome browser and the operating system on the Chromebooks.

An important privacy choice is whether to use Chrome Sync, or not. By default, this Additional Service is disabled. Users and admins can each enable Chrome Sync. Google explains that *"the Chrome Browser and Chrome OS are each consumer products, and are optional ways to access G Suite. Users can choose their own privacy settings¹⁴³ and select which Google features they use in Chrome for more privacy options (for example, [Enhanced] Spellchecker)."¹⁴⁴*

Figures 23 and 24: Default settings Chrome browser¹⁴⁵

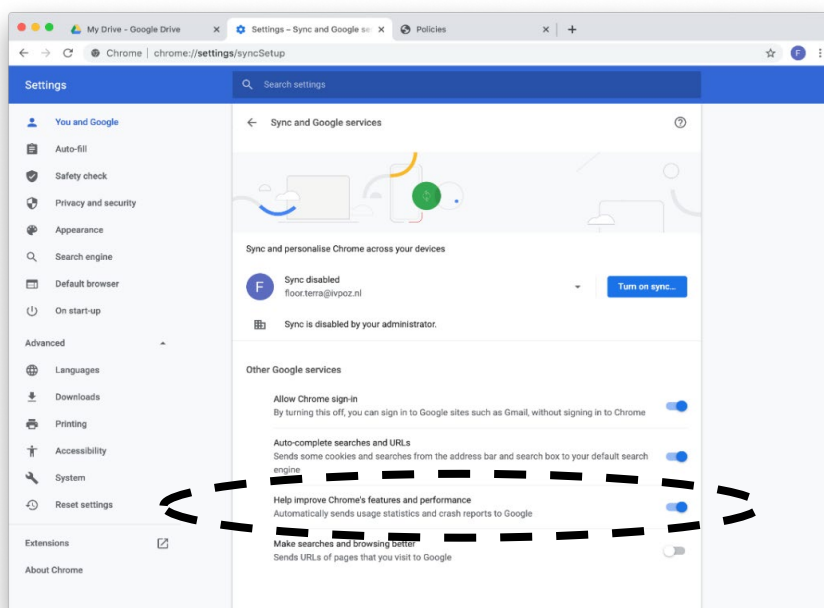


¹⁴² Google, Sign in to multiple accounts at once, URL: <https://support.google.com/accounts/answer/1721977>

¹⁴³ Google Chrome Help, Choose your privacy settings, URL: <https://support.google.com/chrome/answer/114836>

¹⁴⁴ Google Chrome Help, Choose which Google features you use in Chrome, URL: <https://support.google.com/chrome/answer/9116376>

¹⁴⁵ These settings appear to be dynamic. The screenshots were made on 21 June 2020.



By default, the transmission of personal data in crash reports and usage statistics to Google is enabled. The *Enhanced Spellcheck* is disabled in the Chrome browser, but end users can enable it. As explained in Section 1.4.3, admins cannot centrally prevent end users from turning using the *Enhanced Spellcheck*.

3.2 Privacy controls administrators

Administrators of G Suite Enterprise can exercise control over the devices of employees in multiple ways, for example through advanced mobile device management.

For this report, three controls were examined:

1. Access for end users to Additional Services
2. Privacy controls for the Chrome Browser
3. Access to Marketplace apps

These controls are discussed below, in Sections 3.2.1 to 3.2.3.

Section 3.2.4 discusses different types of data processing for which there are no administrator privacy controls.

3.2.1 Access to Additional Services

Access to the Additional Services is enabled by default for G Suite Enterprise. Google explains that it has chosen this setting "to offer a smooth experience to G Suite customers, with no additional charge."¹⁴⁶

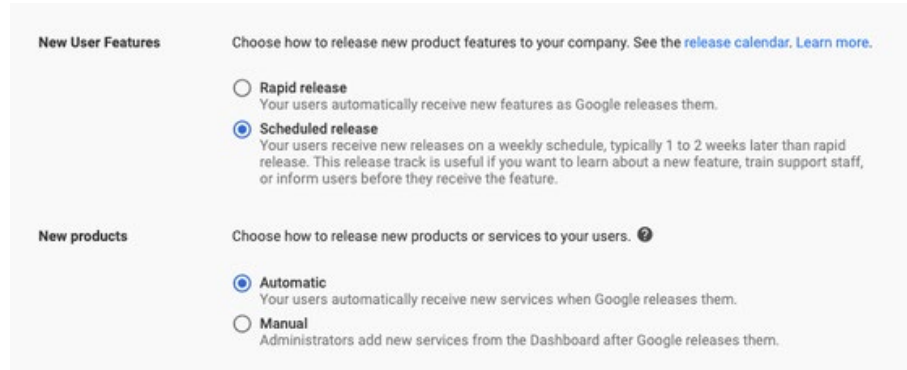
There are currently 53 Additional Services that can be controlled individually, but this list is dynamic and therefore subject to change. Administrators can choose to collectively or individually enable or disable access to those Additional Services. Google warns that the overview of Additional Services, with or without individual controls, is subject to change without notice.¹⁴⁷ Google describes that admins can

¹⁴⁶ Google reply to part A of the DPIA.

¹⁴⁷ Google, G Suite Admin Help, Additional Google services, URL: <https://support.google.com/a/answer/181865?hl=en>

choose how new user features are released to users.¹⁴⁸ As shown in [Figure 25](#) when an administrator has disabled access to all Additional Services and a new Additional Service is added by Google, access to the new service is automatically released to all users, with a delay of 1 to 2 weeks after the introduction.

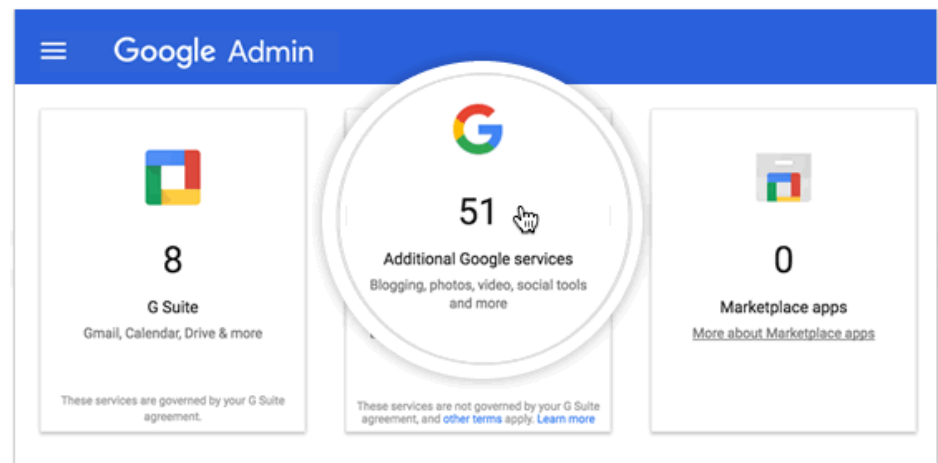
Figure 25: Default setting: automatic release of new features



When Google offers opt-out controls for use of the Additional Services, these controls are granular. A system administrator can turn a specific Additional Service off for all end users, only for a group of end users in an organisational unit, or for a set of end users across or within organisational units.

As examples of Additional Services without an opt-out control, Google mentions Allo, Chromecast and Google Surveys.¹⁴⁹ Admins can only block access to these Additional Services all at once.

Figure 26: Admin overview of 51 additional Google services and Marketplace apps¹⁵⁰



Access to blocked Additional Services

Privacy Company has tested what happens if an admin has turned off an Additional Service, such as Google Search or YouTube, but a G Suite Enterprise end user nevertheless accesses the service. In that case, the end user is silently signed out from the Google Account, and can visit the service as end user without Google Account. Google does not show any warning that the end user has left the G Suite Enterprise environment.

¹⁴⁸ Google, Automatically turn newly released services on or off, URL: <https://support.google.com/a/answer/82691>

¹⁴⁹ Google G Suite Admin Help, Manage services that are not controlled individually, URL: <https://support.google.com/a/answer/7646040>

¹⁵⁰ Idem.

After the Additional Service Search and Assistant was disabled, Google still served personalised ads to the (signed-out) end user. However, these ads were based on the search query, or other contents of that particular browsing session. After searching for baby products, Google Search showed contextual ads in the search engine for nannies and nurseries in The Hague.

Google explained: *"If the Search and Assistant setting is disabled, Search processes queries as if the end user was not authenticated. These G Suite end users may see targeted advertising based on their current session activity but will not be served advertisements based on their use of G Suite or any of their Google Account attributes."*¹⁵¹

As explained in Section 3.1.6, if an employee is simultaneously signed in with a consumer account, Google can process the search data to enrich the Ads Personalization profile of the consumer Google Account.

3.2.2

Privacy controls for the Chrome browser

Administrators can exercise some control over the Chrome browser. In reply to this DPIA, Google frequently points to Chrome Enterprise, but since this is a separate product, not included in G Suite Enterprise, these controls are out of scope of this DPIA. As explained in Section 1.4.3, in G Suite for Enterprise admins cannot block the use of the *Enhanced Spellcheck* in the Chrome browser.

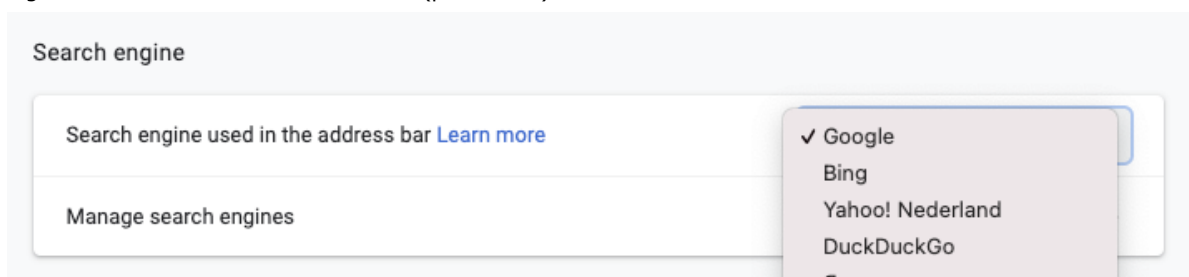
Google explains that the Chrome browser will share location data *'with your default search engine'* by default:

"Chrome won't allow a site to access your location without your permission; however, on mobile devices, Chrome automatically shares your location with your default search engine if the Chrome app has permission to access your location and you haven't blocked geolocation for the associated web site. Chrome uses Google Location Services to estimate your location. The information that Chrome sends to Google Location Services may include:

*The Wi-Fi routers closest to you
Cell IDs of the cell towers closest to you
The strength of your Wi-Fi or cell signal
The IP address that is currently assigned to your device."*¹⁵²

The default search engine is Google Search as shown in [Figure 27](#).¹⁵³

Figure 27: Default browser in Chrome (pre-ticked)



¹⁵¹ Google response 5 June 2020.

¹⁵² Google Chrome Privacy Notice, Last modified: 20 May 2020, URL: https://www.google.com/chrome/privacy/?hl=en_GB

¹⁵³ As tested repeatedly by Privacy Company in a new clean install of a Chrome browser.

Administrators have the ability to apply policies to managed Chrome browsers and Chromebooks. Google explains in its Chrome Privacy Notice:

"Chrome contacts Google to check for these policies when an end user first starts browsing (except in guest mode). Chrome checks periodically for updates to policies. An administrator can set up a policy for status and activity reporting for Chrome, including location information for Chrome OS devices. Your administrators may also have the ability to access, monitor, use or disclose data accessed from your managed device."¹⁵⁴

3.2.3

Access to Marketplace apps

The G Suite Marketplace is an app store. Anyone with a Google Account can download apps relating to G Suite from the Marketplace. These apps are called *add-ins*. By default, Google allows G Suite Enterprise end users to install all available add-ins from the G Suite Marketplace.¹⁵⁵ If those add-ins want to access the G Suite Customer Data (which is almost always the case), the end user can easily give such an app access in the same way as authorising any other website for single sign-on, via OAUTH or SAML.

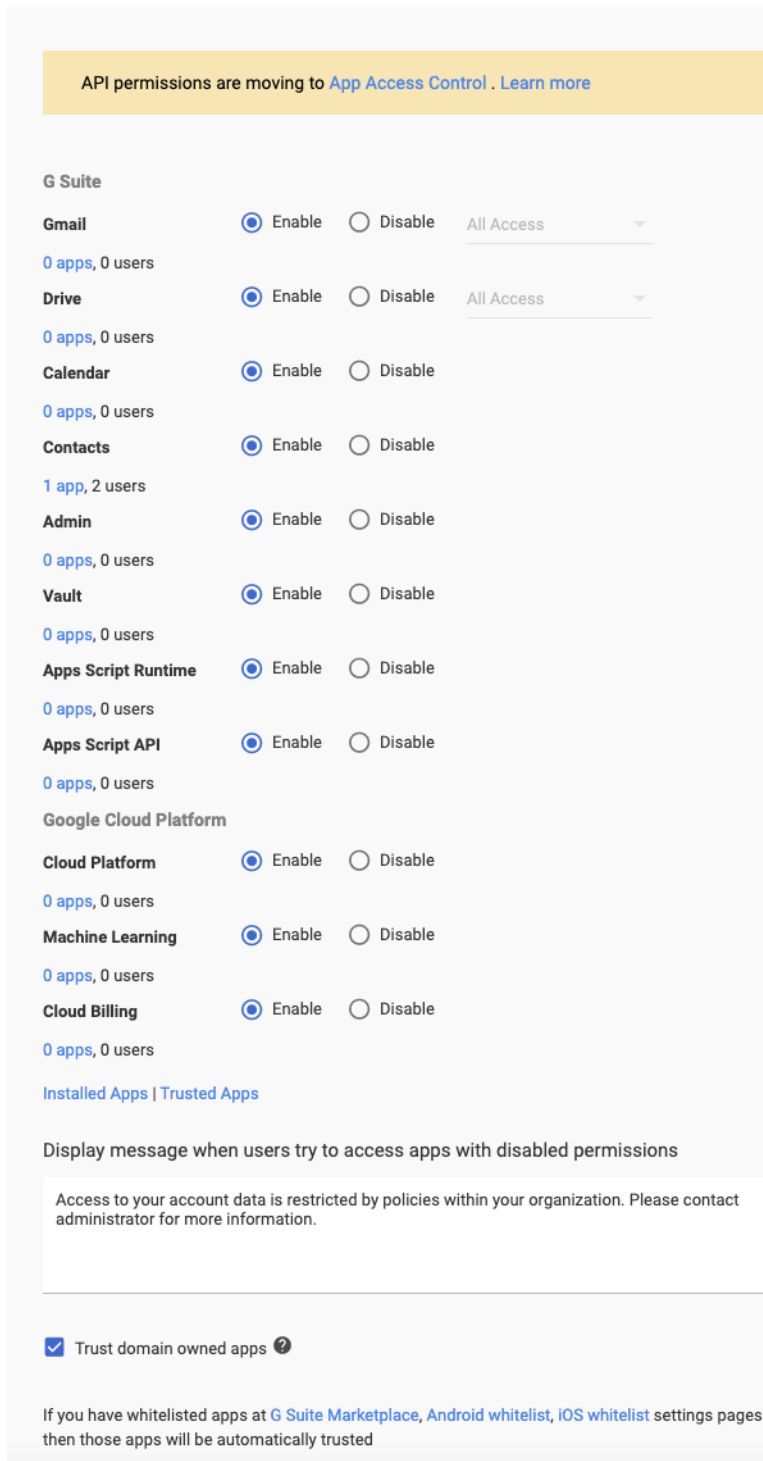
Administrators have three choices in managing the G Suite Marketplace. They can prohibit the installation of all apps, allow only whitelisted apps, or allow everything. The default setting of installed Marketplace apps is that access to Customer Data is enabled by default. Administrators can centrally disable this access, and can also give each app restricted or unrestricted access to Customer Data (See [Figure 28](#) below).

If administrators allow employees to install (whitelisted) apps, they have only limited control over that app's access to Customer Data. The available control only allows for a Yes or No choice. Google does not provide a more granular control over the different kinds of permissions that the app needs, such as access to contacts, to camera, etcetera.

¹⁵⁴ Ibid.

¹⁵⁵ See: <https://gsuite.google.com/marketplace>

Figure 28: Default settings Marketplace: all access is allowed



After installation by the end-user, administrators can see that the end user has installed the app, and what permissions that app requires.

Figure 29: Default setting: unrestricted access to Customer Data

Service	Access	Allowed Apps	Users
Drive	Unrestricted	0	0
Gmail	Unrestricted	0	0
Calendar	Unrestricted	0	0
Contacts	Unrestricted	0	0
G Suite Admin	Unrestricted	0	0
Vault	Unrestricted	0	0
Cloud Platform	Unrestricted	0	0
Cloud Billing	Unrestricted	0	0
Cloud Machine Learning	Unrestricted	0	0
Apps Script Runtime	Unrestricted	0	0

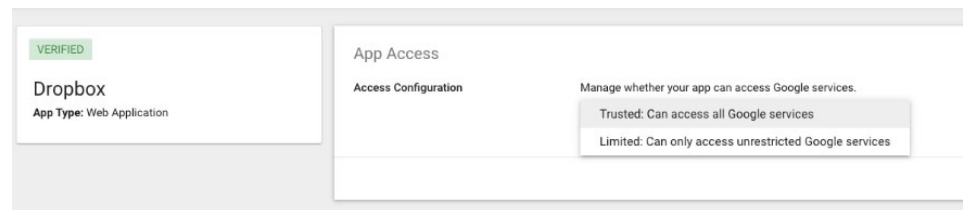
3.2.4

Access rights for external apps and sites via Single Sign-in

For this DPIA, a test user authorised the third-party service Dropbox with single sign-in. In this case Dropbox requested two permissions: for 'Context', and 'Other'. Single sign-on is enabled by default for end users.

As shown in Figure 30 below, admins can change the default setting of full access to all Google services, to limited access, to unrestricted Google services. The default setting is that access to all Google services is unrestricted, so this setting by itself does not immediately limit access to Customer Data.

Figure 30: Changing access rights per app from full access to limited access



3.2.5

Missing central privacy controls for administrators

This DPIA identifies five scenarios where administrators of G Suite Enterprise should be able to exercise central privacy control, but where such a control is not available.

Admins cannot:

1. Prevent use of *Enhanced Spellcheck* in Chrome;
2. Prevent reuse of Customer Data through *Spelling and grammar* for machine learning;
3. Limit the collection of telemetry data and other Diagnostic Data;
4. Change the default setting for Ads Personalization; and
5. Prohibit the use of services for which Google is the data controller, such as Feedback.

Section 2.3 and [Figure 15](#) describe how content from files that Google obtains as Customer Data may end up in the telemetry data (Diagnostic Data) as a result of the use of the **Enhanced Spellcheck** in the Chrome browser. Admins can only centrally block this traffic if they separately procure Chrome Enterprise (not part of the G Suite Enterprise offering, out of scope of this DPIA).

As quoted in Section 1.4, Google explains it uses *machine learning* that commonly uses *billions of common phrases and sentences* as language understanding models. This means Google permits itself to process Customer Data for a purpose not specifically agreed by the customer. There is no opt-out for government organisations.¹⁵⁶

As described in Section 2.3.1, Google collects **detailed telemetry data** (Diagnostic Data) from Android devices, the Chrome OS and the Chrome browser. It is plausible that Google collects similar data from iOS devices.

Section 4.4 describes that the Chrome OS and browser also install three unique identifiers, for installation tracking, tracking of promotional campaigns and field trials. Admins have no control over this data collection and these trackers, and cannot block or limit Google from collecting these personal data.

Google does not allow admins to **change the default setting for Ads Personalization**. Google explained that admins should block the Additional Services, or encourage end users to individually turn Ads Personalization off.

*"We would recommend that the Additional Services are switched off as a solution to this issue. However, if the Dutch Government wishes to allow their end users to access Additional Services while logged into their corporate account, without receiving personalised ads, then end users should be advised to switch Ads Personalization off in 'My Account'."*¹⁵⁷

Finally, admins cannot centrally prevent end users from using **controller services such as Feedback** that are embedded in the Core Services.

4. Purposes of the processing

Under the GDPR, the principle of 'purpose limitation' dictates that personal data may only be collected for specified, explicit and legitimate purposes, and may not be further processed in a manner that is incompatible with the initial purpose.¹⁵⁸ The purposes are qualified and assessed in part B of this DPIA. This Section provides a factual description of the purposes of the processing of Customer Data and Diagnostic Data by government organisations and Google.

4.1 Purposes government organisations

The general interests government organisations may have to use G Suite Enterprise are described in Section 6.1.

Government organisations may process Diagnostic Data collected by Google about the individual use of the G Suite services when accessing or retrieving data from the available audit log files. Government organisations may need to process these data to comply with information security requirements, to verify access authorisations, to investigate and mitigate data security breaches and to comply with data subject right requests.

As data controllers, government organisations must determine when they need to access log files generated by Google, what retention periods are necessary to comply with security requirements, and for what specific purposes specific personal data in

¹⁵⁶ After completion of this report, Google has provided guarantees that it will not use grammar and spelling outside of the domain of each Enterprise customer to improve spelling suggestions.

¹⁵⁷ Idem.

¹⁵⁸ Article 5(1)(b) GDPR.

the log files may be (further) processed and analysed. Their specific purposes are not in scope of this umbrella DPIA.

4.2 Purposes Google

As will be analysed in Section 5, Google considers itself to be a data processor for the processing of personal data in Customer Data from the Core Services, the Features, the Google Account (to the extent used in conjunction with a Core Service) and the Technical Support Services. Section 4.2.1 discusses the purposes described in the G Suite DPA, the data processing agreement between the government organisation and Google and purposes identified by Privacy Company on the basis of the G Suite DPA, other Google documentation, responses from Google and technical findings of this DPIA.

Google considers itself to be an independent data controller for the processing of personal data actively provided by end users in (a) the Additional Services, (b) the Google Account (to the extent not used in conjunction with a Core Service) and (c) Feedback and possible Other related services. Google also considers itself to be an independent data controller for the processing of all Diagnostic Data, including about the use of the Core Services and about the use of the Technical Support Services.

At the time of completion of this DPIA, Google only described the purposes of its processing of personal data as a data controller in its (consumer) Privacy Policy.¹⁵⁹ These purposes are discussed in Sections 4.2.2.

4.2.1 Purposes personal data in Core Services, Features and the Google Account when used in conjunction with the Core Services

The G Suite DPA contains the following descriptions of the purposes for which personal data in Customer Data from the Core Services are processed:

"Google will process Customer Personal Data *for the purposes of providing the Services and TSS to Customer* in accordance with the Data Processing Amendment."¹⁶⁰

"Customer instructs Google to process Customer Personal Data only in accordance with applicable law:

- to provide the Services and TSS)*
- as further specified via Customer's and End Users' use of the Services (including the Admin Console and other functionality of the Services) and TSS;*
- as documented in the form of the applicable Agreement, including this Data Processing Amendment; and*
- as further documented in any other written instructions given by Customer and acknowledged by Google as constituting instructions for purposes of this Data Processing Amendment."¹⁶¹*
- "For clarity, Google will not process Customer Personal Data for Advertising purposes or serve Advertising in the Services."¹⁶²*

In the context of this DPIA, Privacy Company asked Google to specify what 'providing the Services and TSS' constitutes. Google did not provide any further description other than: **"according to the documented instructions of our customer as a**

¹⁵⁹ On 12 November 2020 Google published a Google Cloud Privacy Notice with a list of purposes. Google, URL: <https://cloud.google.com/terms/cloud-privacy-notice>

¹⁶⁰ Appendix 1 G Suite DPA.

¹⁶¹ Clause 5.2.1 G Suite DPA.

¹⁶² Clause 5.2.2 G Suite DPA.

data controller, which are set out in the section of the DPA entitled "Customer's Instructions".

Google added: "In the same section, Google commits to not process Customer Personal Data other than as instructed."¹⁶³

Google mentions in the G Suite DPA that it secures the Customer Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access, including by encrypting personal data and by helping to restore timely access to personal data following an incident.¹⁶⁴

In Appendix 2 to the G Suite DPA, Google describes the applicable security measures. This description includes a number of scenarios where Google may process Customer Data (including personal data) specifically for the purpose of security.

"Intrusion Detection. Intrusion detection is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents. Google's intrusion detection involves:

- 1. tightly controlling the size and make-up of Google's attack surface through preventative measures;*
- 2. employing intelligent detection controls at data entry points; and*
- 3. employing technologies that automatically remedy certain dangerous situations.*

Incident Response. Google monitors a variety of communication channels for security incidents, and Google's security personnel will react promptly to known incidents.

Encryption Technologies. Google makes HTTPS encryption (also referred to as SSL or TLS connection) available. Google servers support ephemeral elliptic curve Diffie-Hellman cryptographic key exchange signed with RSA and ECDSA. These perfect forward secrecy (PFS) methods help protect traffic and minimize the impact of a compromised key, or a cryptographic breakthrough.

(.)

Infrastructure Security Personnel. Google has, and maintains, a security policy for its personnel, and requires security training as part of the training package for its personnel. Google's infrastructure security personnel are responsible for the ongoing monitoring of Google's security infrastructure, the review of the Services, and responding to security incidents.

(.)

(b) Decommissioned Disks and Disk Erase Policy.

Disks containing data may experience performance issues, errors or hardware failure that lead them to be decommissioned ("Decommissioned Disk"). Every Decommissioned Disk is subject to a series of data destruction processes (the "Disk Erase Policy") before leaving Google's premises either for reuse or destruction. Decommissioned Disks are erased in a multi-step process and verified complete by at least two independent validators. The erase results are logged by the Decommissioned Disk's serial number for tracking. Finally, the erased Decommissioned Disk is released to inventory for reuse and redeployment. If, due

¹⁶³ Google reply to part A of the DPIA.

¹⁶⁴ G Suite DPA, Appendix 1: Google's provision of the Services and TSS to Customer. "Google will implement and maintain technical and organizational measures to protect Customer Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access as described in Appendix 2 (the "Security Measures"). The Security Measures include measures to encrypt personal data; to help ensure ongoing confidentiality, integrity, availability and resilience of Google's systems and services; to help restore timely access to personal data following an incident; and for regular testing of effectiveness. Google may update the Security Measures from time to time provided that such updates do not result in the degradation of the overall security of the Services."

to hardware failure, the Decommissioned Disk cannot be erased, it is securely stored until it can be destroyed."

With respect to Intrusion Detection and Incident Response, like any other service provider Google keeps logs in Google's own monitoring files (SIEM). Such logs may include personal data in Customer Data.

According to Google, these security purposes are not (sub)purposes, because *"they are processing activities carried out to fulfil the instruction to provide G Suite services subject to the contractual security safeguards specified in Appendix 2 of the DPA."*¹⁶⁵

Second, the G Suite DPA states that Google performs *regular testing of effectiveness* of security measures.¹⁶⁶ In the absence of further information, it cannot be excluded that these tests involve the processing of personal data in Customer Data. Testing must be regarded as a separate purpose, as the testing of measures is distinctively different from applying the measures. In reply to this DPIA Google explained that Customer Personal Data are not used to test security measures.

Third, in the G Suite DPA and TSS guidelines Google describes the processing of Customer Personal Data for Technical Support services. As described in Section 1.4.4, Google explained: *"Google remains a data processor in respect of Customer Personal Data accessed by Support agents in order to provide support."*

Another purpose referred to in the G Suite DPA, is processing to comply with obligations under applicable law.¹⁶⁷ This type of disclosure will be discussed in more detail in Section 5.3.7 of this report.

Google documentation and responses

In a G Suite security whitepaper, Google explains: *"Google indexes customer data to provide beneficial services, such as spam filtering, virus detection, spellchecker and the ability to search for emails and files within an individual account."*¹⁶⁸ In response to questions from Privacy Company, Google confirmed that it processes personal data in Customer Data to detect, prevent or address spam, malware and illegal activity.¹⁶⁹

According to Google, the processing of personal data for security purposes and the detection of spam, malware and illegal activity is *compatible* with the main purpose of providing the service.

Google writes:

*"The processing of Customer Personal Data to provide secure G Suite services is compatible with the customer's instructions (as documented in the G Suite DPA and as required by the GDPR), and should not be seen as a distinct purpose of processing Google permits for itself."*¹⁷⁰

¹⁶⁵ Google reply to part A of the DPIA.

¹⁶⁶ Clause 7.1.1 G Suite DPA.

¹⁶⁷ Clause 5.2.2 G Suite DPA.

¹⁶⁸ Google Cloud Security and Compliance, Data Usage, No advertising in G Suite, URL: <https://gsuite.google.com/learn-more/security/security-whitepaper/page-6.html#our-philosophy>.

¹⁶⁹ From responses provided by representatives of Google to SLM Microsoft Rijk during the course of the DPIA.

¹⁷⁰ Google reply to part A of this DPIA.

With regard to the detection of illegal activity, Google refers to an online form that administrators can use to report abuse incidents.¹⁷¹ Google also explains it may also identify known abuse content itself. "For example, Google will block the sharing of viruses and malware within Google Drive based on industry standard scanning practices which rely on recognition of suspect 'signatures' and characteristics."¹⁷²

On its public help page about uploading files to Google Drive, Google writes: "Google Drive scans a file for viruses before the file is downloaded or shared. If a virus is detected, end users cannot convert the infected file to a Google Doc, Sheet, or Slide, and they'll receive a warning if they attempt these operations. (...) All Google Drive files, including uploaded or converted files, follow the same program policy. [Learn more](#)."¹⁷³

The hyperlinked words [Learn More](#) link to a page with 13 different program policies applicable to consumer services. For G Suite Enterprise, the only relevant policy is the G Suite Acceptable Use Policy.¹⁷⁴ This policy lists customer compliance obligations, but does not mention pro-active analysis by Google.

The technical findings of this DPIA show that Google also uses Customer Data from the Core Services to improve its products and services. As described in Section 1.4, Google uses Customer Data from Core Services to improve the Feature *Spelling and Grammar* through machine learning.¹⁷⁵

After questions from Privacy Company, Google provided further details about the purposes of the processing. Google requested that this information remain confidential.

In sum, Google processes personal data from the Core Services for the following purposes:

1. Transmitting (technically delivering) the Core Services;
2. Providing Technical Support Services;
3. Securing the services;
4. Proactively scanning, detecting and addressing viruses, malware and spam;
5. Improving the services, such as by using machine learning to improve the Feature *Spelling and Grammar*.¹⁷⁶
6. To comply with obligations under applicable law.

4.2.2 *Purposes Diagnostic Data and Account Data from the Core Online Services*

As further explained in Sections 1.5 and 5.3 of this report, Diagnostic Data are not included in the scope of the G Suite DPA. Google has not published any documentation about the purposes for which it processes Diagnostic Data from the Core Services.

¹⁷¹ Google, Reporting Abuse Incidents, URL:

<https://support.google.com/a/answer/134413?hl=en>

¹⁷² From responses provided by representatives of Google to SLM Microsoft Rijk during the course of the DPIA.

¹⁷³ Google, upload files to Google Drive, bottom of the page under 'Security', URL:

<https://support.google.com/a/answer/172541?hl=en>

¹⁷⁴ G Suite Acceptable Use Policy, URL:

https://gsuite.google.com/intl/en/terms/use_policy.html

¹⁷⁵ Google, Correct your spelling & grammar in Google Docs, URL:

<https://support.google.com/docs/answer/57859?hl=en> After completion of this report, Google provided guarantees it will not use any spelling and grammar data to improve the spelling services outside of the domain of each Enterprise customer.

¹⁷⁶ After completion of this DPIA, Google provided guarantees that it will not use machine learning to improve spelling and grammar outside of the domain of each Enterprise customer.

In reply to part A of this DPIA, Google provided 8 purposes.

1. *"Providing the services;*
2. *Providing technical support*
3. *Improving the services, based on aggregate usage information;*
4. *Keeping the service up-to-date (providing automatic product updates);*
5. *Providing secure services*
6. *Communicating with our customers and their admins [Contact Data];*
7. *Managing G Suite accounts (including billing and financial records);*
8. *Complying with applicable law."*¹⁷⁷

The purpose of 'improving the services' is also explicitly mentioned by Google in relation to the collection of telemetry data from Android devices: *"The data is analyzed and used to improve products, hardware, and services."*¹⁷⁸

After questions from Privacy Company, Google provided further details about these purposes of the processing. Google requested that this information remain confidential.

Based on public documentation quoted above, Google also processes the Diagnostic Data for the following purpose:

9. Proactively scanning, detecting and addressing viruses, malware and spam

As outlined in Section 2.3, Google sets a DoubleClick cookie if a non-authenticated end user visits a log-in page for the G Suite Core Services: to determine if an end user is eligible for personalised ads, or if the end user is a child.

This purpose of the processing of the cookie Diagnostic Data is not mentioned in Google's public documentation about DoubleClick cookies. Google writes: *"We also use one or more cookies for advertising we serve across the web. One of the main advertising cookies on non-Google sites is named 'IDE' and is stored in browsers under the domain doubleclick.net. Another is stored in google.com and is called ANID. We use other cookies with names such as DSID, FLC, AID, TAID, and exchange_uid. Other Google properties, like YouTube, may also use these cookies to show you more relevant ads."*¹⁷⁹

It follows from this public information that Google processes the Diagnostic Data for a tenth purpose:

10. Determining the account status and ads personalization preferences [cookies];

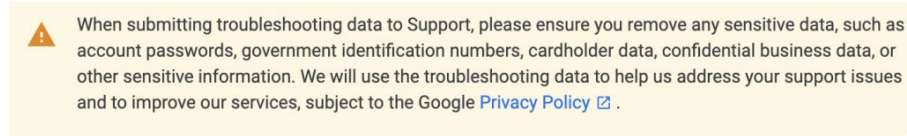
When administrators submit troubleshooting data to Google's support department, they are warned that they should remove sensitive information, because Google can process these data as a data controller, for the purposes of its (consumer) Privacy Policy.

¹⁷⁷ Google reply to part A of the DPIA.

¹⁷⁸ See Section 2.3.1 of this report.

¹⁷⁹ Google, Types of cookies used by Google, URL: <https://policies.google.com/technologies/types?hl=en-US>

Figure 31: Screenshot provided by Google



This reference from Google to its (consumer) Privacy Policy means it qualifies itself as a data controller, and not as a data processor. It is not clear why Google does not act as a data processor for the purpose of addressing support issues.

[CONFIDENTIAL]

Google considers all information about the purposes of processing Diagnostic Data provided during the course of this DPIA confidential. Google has committed to create "an Enterprise Privacy Notice that will provide clarification of the purposes for which we process personal information that Google collects or generates that is not Customer Data." At the time of completion of this DPIA, no timeline was provided. In 12 November 2020, Google published a Google Cloud Privacy Notice with a list of purposes.¹⁸⁰

Table 10: Purposes Customer Data and Diagnostic Data Core Services

Customer Personal Data	Other personal data (Diagnostic Data)
Transmitting / providing the service	
Providing Technical Support Services	
Complying with applicable law	
Providing secure services	
Proactively scanning, detecting and addressing viruses, malware and spam	
Improving the services, such as using machine learning to improve the Feature <i>Spelling and Grammar</i>	Improving the services, based on aggregate usage information
	Communicating with customers and admins [Account]
	Managing G Suite accounts (including billing and financial records)
	Keeping the service up-to-date
	Determining the account status and ads personalisation preferences [Cookie Data]

4.2.3

Possible additional purposes for Customer Data and Diagnostic Data

Google does not provide a limitative list of purposes for the processing of the Customer Data, the Diagnostic Data, Account Data and other data about the use of the G Suite Core Services such as cookie and website data.

Therefore this DPIA examines the more detailed description of purposes provided in Google's (consumer) Privacy Policy. Since there is only one Google Account, and data from the Core Services are linked to Additional Services in the same back-end infrastructure, some of the purposes mentioned in the (consumer) Privacy Policy could very well apply to the Diagnostic Data collected through the use of the Core Services, because Google does not explicitly and publicly exclude such purposes.

¹⁸⁰ Google Cloud Privacy Notice, 7 December 2020, URL: <https://cloud.google.com/terms/cloud-privacy-notice>

Different from the personal data in Customer Data, Google does not exclude the use of Diagnostic Data for advertising purposes in the G Suite DPA or other relevant contractual documents.

[CONFIDENTIAL]

Possible purposes for the processing of personal data in Customer Personal Data and the Diagnostic Data that are not contractually excluded, are listed below. The key difference is that Google does exclude the use of advertising purposes for the personal data in Customer Data, but not for Diagnostic Data. That is why advertising purposes are quoted between brackets, to indicate they only apply to the Diagnostic Data.

1. **Help end users share content** by suggesting recipients from their contacts;
2. **Maintaining the service by tracking outages;**
3. **Provide recommendations** *For example, Security Check-up provides security tips adapted to how you use Google products;*
4. **Provide personalised content**, *for example based on information like apps you've already installed (...) to suggest new apps you might like;*
5. **Customizing our services** *to provide you with a better end user experience, provide customised search results;*
6. **Optimize product design**, *For example, we analyze data about your visits to our sites to do things like optimize product design;*
7. **Communicate with you to interact with you directly.** *For example, we may send you a notification if we detect suspicious activity;¹⁸¹*
8. **Improve the reliability of our services.** *We use automated systems that analyze your content to provide you with things like customized search results, [personalized ads], or other features tailored to how you use our services;*
9. **Use cookies for many purposes.** *We use them, for example, to remember your safe search preferences, [to make the ads you see more relevant to you'], to count how many visitors we receive to a page, to help you sign up for our services, to protect your data, or to remember your ad settings.¹⁸²;*
10. **To allow specific partners to collect information from your browser or device** *for [advertising] and measurement purposes using their own cookies or similar technologies;*
11. **When necessary for legitimate business or legal purposes** *such as financial record-keeping;*
12. **Other purposes not covered in the Privacy Policy**, we'll ask for your consent.

In sum, this DPIA identifies 6 purposes for which Google processes personal data in Customer Data and 10, sometimes different, purposes for which Google processes Diagnostic Data from the Core Services. Given the lack of transparency about what Google qualifies as 'Provide the Services and TSS', it cannot be excluded that Google processes personal data and Diagnostic Data from the Core Services for 12 other purposes. For the avoidance of doubt, the purposes listed in this Section 4 only describe the factual findings of this DPIA. The assessment of whether these purposes are specific and explicit is made in Section 13.

¹⁸¹ According to Google, this relates to the use of contact data. It is still included in this list because it is plausible that Google will use Diagnostic Data to detect suspicious activity.

¹⁸² Google, How Google uses cookies, URL: <https://policies.google.com/technologies/cookies?hl=en>

4.3 **Purposes Additional Services and Google Account, when not used in a Core Service**

The processing of personal data in connection with Additional Services is explicitly excluded from the scope of the G Suite DPA.

Google explains that its consumer Terms of Service and its (consumer) Privacy Policy apply to such processing:

*"For clarity, this Data Processing Amendment does not apply to the processing of personal data in connection with the provision of any Additional Products installed or used by Customer, including personal data transmitted to or from such Additional Products. Customer may use the functionality of the Services to enable or disable Additional Products, and is not required to use Additional Products in order to use the Services."*¹⁸³

Google explains in its Privacy Policy:

*"This Privacy Policy applies to all of the services offered by Google LLC and its affiliates, including YouTube, Android, and services offered on third-party sites, such as advertising services. This Privacy Policy doesn't apply to services that have separate privacy policies that do not incorporate this Privacy Policy."*¹⁸⁴

The Terms of Service and the (consumer) Privacy Policy also apply to the processing in connection with the Google Account. Google explains: *"When you're signed in, we also collect information that we store with your Google Account, which we treat as personal information."*¹⁸⁵

As described in Section 1.4.2 of this DPIA, Google explained that personal data relating to the Google Account are processed in the same way as Core Services when its functionality is used in conjunction with Core Services. Taking into account this distinction, Google should only process personal data relating to the Google Account under its (consumer) Privacy Policy if the Google Account is used with an Additional Service or Other related service such as Feedback, when Google acts as a data controller.

However, this technical distinction in the processing of Google Account Data is not contractually guaranteed, nor publicly documented.

In its (consumer) Privacy Policy, Google explains that it may personal data for a multitude of purposes. Google frequently uses the words 'for example' (25 times) and like (33 times).

To get a clear picture of the purposes included in the (consumer) Privacy Policy, all purposes and examples that Google lists are enumerated separately below as distinct purposes.

Google does not specify what categories of personal data it may process for each purpose.

The 33 purposes are:

1. **Providing our service**
2. **Help end users share content** by suggesting recipients from their contacts.
3. **Maintaining the service by tracking outages**
4. **Troubleshooting end user reported issues**

¹⁸³ G Suite DPA, Section 5.3.

¹⁸⁴ Google Privacy Policy, When this policy applies, URL: <https://policies.google.com/privacy?hl=en-US#about>

¹⁸⁵ Google Privacy Policy, We want you to understand the types of information we collect as you use our services, URL: <https://policies.google.com/privacy?hl=en-US>

5. **Make improvements to the services**, for example *understanding which search terms are most frequently misspelled helps us improve spell-check features used across our services*. This purpose is also described in a slightly different way later in the Privacy Policy as: *"Understanding how people use our services to ensure and improve the performance of our services"*
6. **Develop new products and features** *that are useful for our end users*
7. **Provide recommendations** *For example, Security Check-up provides security tips adapted to how you use Google products*
8. **Provide personalised content**, for example *based on information like apps you've already installed and videos you've watched on YouTube to suggest new apps you might like*
9. **Customizing our services** *to provide you with a better end user experience, provide customised search results*
10. **Providing advertising** *which keeps many of our services free (and when ads are personalized, we ask for your consent)*
11. **Show personalized ads** *based on your interests. For example, if you search for "mountain bikes," you may see an ad for sports equipment when you're browsing a site that shows ads served by Google.*
12. **Share information that personally identifies you with advertisers**, such as your name or email, only if you ask us to. *For example, if you see an ad for a nearby flower shop and select the "tap to call" button, we'll connect your call and may share your phone number with the flower shop.*
13. **Create analytical data** *to*
14. **Optimize product design**, *For example, we analyze data about your visits to our sites to do things like optimize product design*
15. Enable advertisers to **combine information with Google Analytics**, *When you visit sites that use Google Analytics, Google and a Google Analytics customer may link information about your activity from that site with activity from other sites that use our ad services.*
16. **Use data for measurement**, *for example data about the ads you interact with to help advertisers understand the performance of their ad campaigns.*
17. **Communicate with you to interact with you directly**. *For example, we may send you a notification if we detect suspicious activity,*
18. **Inform you** *about upcoming changes or improvements to our services.*
19. **Marketing** *to inform end users about our services*
20. **Provide support if you contact Google**, *to help solve any issues you might be facing.*
21. **Improve the safety of our services**. *This includes detecting, preventing, and responding to fraud, security risks, and technical issues that could harm Google, our end users, or the public.*
22. **Detect abuse** *such as spam, malware, and illegal content by analyzing your content*
23. **Protecting against harm to the rights, property or safety of Google, our end users, or the public** *as required or permitted by law, including [also slightly differently defined as: "Fulfilling obligations to our partners like developers and rights holders AND Enforcing legal claims, including investigation of potential violations of applicable Terms of Service]*
24. **Disclosing information to government authorities** *Also slightly differently defined as: "To respond to legal process or an enforceable governmental request."*
25. **Improve the reliability of our services**. *We use automated systems that analyze your content to provide you with things like customized search results, personalized ads, or other features tailored to how you use our services.*
26. **Use algorithms to recognize patterns in data**. *For example, Google Translate helps people communicate across languages by detecting common language patterns in phrases you ask it to translate.*

27. **Combining information among all services and across devices to improve Google's services and the ads delivered by Google**, *For example, if you watch videos of guitar players on YouTube, you might see an ad for guitar lessons on a site that uses our ad products. 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.*
28. **Help other end users identify you**, *If other end users already have your email address or other information that identifies you, we may show them your publicly visible Google Account information, such as your name and photo.*
29. **Use cookies for many purposes**. *We use them, for example, to remember your safe search preferences, to make the ads you see more relevant to you, to count how many visitors we receive to a page, to help you sign up for our services, to protect your data, or to remember your ad settings.*¹⁸⁶
30. **To allow specific partners to collect information from your browser or device** *for advertising and measurement purposes using their own cookies or similar technologies*
31. **Performing research**, *Performing research that improves our services for our end users and benefits the public*
32. **When necessary for legitimate business or legal purposes** *such as security, fraud and abuse prevention, or financial record-keeping.*
33. **Other purposes not covered in this Privacy Policy**, *we'll ask for your consent, for example, to*
 - a. Collect your voice and audio activity for speech recognition.
 - b. Use Location History if you want traffic predictions for your daily commute
 - c. Use YouTube Watch History to get better video suggestions.
 - d. if you use Google Home to make a reservation through a booking service, we'll get your permission before sharing your name or phone number with the restaurant.
 - e. Process your payment information when you buy extra storage for Google Drive.

[CONFIDENTIAL]

4.4 Specific purposes Chrome OS and the Chrome browser

As explained in Section 1.4.3 of this report, ChromeOS and the Chrome browser are services with shared separate terms and a separate Privacy Notice. In this privacy policy Google mentions specific purposes for the processing of personal data.¹⁸⁷ Most of these purposes are purely technical, and only relevant for the functioning of a web browser, but other purposes could come as a surprise for end users, for example the collection of detailed location information from mobile devices when using the pre-ticked default Google search engine.

The purposes in the Chrome privacy policy are:

- Store web surfing data in your Google Account by turning on Sync;
- Send standard log information to all sites you visit, including your IP address and data from cookies;
- **Use cookies** to deliver the services, personalize adds and analyze traffic;
- Intercepting man in the middle types of suspicious activity;
- Pre-rendering the sites you visit;

¹⁸⁶ Google, How Google uses cookies, URL:

<https://policies.google.com/technologies/cookies?hl=en>

¹⁸⁷ Google Chrome Privacy Notice, last modified 20 May 2020, URL:

https://www.google.com/chrome/privacy/?hl=en_GB

- **Share the location from mobile devices with Google** if you use Google Search, or with third parties if the end user consents, and send the following information:
 - The Wi-Fi routers closest to you;
 - Cell IDs of the cell towers closest to you;
 - The strength of your Wi-Fi or cell signal;
 - The IP address that is currently assigned to your device;
- Send information to Google to check for updates, get connectivity status, estimate the number of active end users;
- Send URLs of some pages you visit to Google *when your security is at risk*;
- Storing all queries in Google Search in your Google Account;
- **Predict the word(s) end users want to search for**, even before hitting enter in the Search engine, based on the individuals browsing history and what other people are looking for;
- Sending limited anonymous information about web forms to **improve Autofill**;
- **Process payment information** and share with Google Pay;
- **Customize your language** based on the languages of sites you visit;
- **Send usage statistics and crash reports** to Google;
- Share aggregated, non-personally identifiable information publicly and with partners – like publishers, advertisers or web developers;
- **Send a unique Adobe Flash identifier** to content partners and websites that use Adobe Flash Access;
- Provide **access to Additional Services** such as Google Translate
- Install three kinds of unique identifiers and use these for:
 - Installation tracking;
 - Tracking of promotional campaigns;
 - Field trials.

The Chrome privacy notice contains specific explanations about the processing of Diagnostic Data; for the purposes of *Usage Statics and crash reports* and *Server Log Privacy Information*.

Google explains that Chrome OS and the Chrome browser usage statistics contain information such as preferences, button clicks, performance statistics, and memory usage. Usage data may also include web page URLs or personal data, if the setting is enabled: "*Make searches and browsing better / Sends URLs of pages you visit to Google.*"¹⁸⁸ As shown in [Figure 25](#), this option is disabled by default in the tested Chrome browser.

Additionally, Google explains: "*If Google Play apps are enabled on your Chromebook and Chrome usage statistics are enabled, then Android diagnostic and usage data is also sent to Google.*"¹⁸⁹ As shown in [Figure 25](#) the sending of usage statistics is enabled by default.

5. Processor or (joint) controller

This section assesses the data protection role of Google and government organisations in the context of the G Suite Enterprise services.

¹⁸⁸ Google Chrome help, Start or stop automatically reporting errors and crashes, <https://support.google.com/chrome/answer/96817> On desktops, this option can be found in the Chrome settings You and Google, 'Sync and Google Services'.

¹⁸⁹ Google Chrome Privacy Notice, Section *Usage statistics and crash reports*.

5.1 Definitions

The GDPR contains definitions of the different roles of parties involved in processing data: (joint) controller, processor and subprocessor.

Article 4(7) of the GDPR defines the (joint) controller as:

"the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law."

Article 26 of the GDPR stipulates that where two or more data controllers jointly determine the purposes and means of a processing, they are joint controllers. Joint controllers must determine their respective responsibilities for compliance with obligations under the GDPR in a transparent manner, especially towards data subjects, in an arrangement between them.

Article 4(8) of the GDPR defines a processor as:

"a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller." A subprocessor is a subcontractor engaged by a processor that assists in the processing of personal data on behalf of a data controller.

Article 28 GDPR sets out various obligations of processors towards the controllers for whom they process data. Article 28(3) GDPR contains specific obligations for the processor. Such obligations include only processing personal data in accordance with documented instructions from the data controller and cooperating with audits by a data controller. Article 28(4) GDPR stipulates that a data processor may use subprocessors to perform specific tasks for the data controller, but only with the prior authorisation of the data controller.

When data protection roles are assessed, the formal contractual division of roles is not leading nor decisive. The actual role of a party must primarily be determined on the basis of factual circumstances.

5.2 Data processor

5.2.1 Personal data in Customer Data in the Core Services

Pursuant to the G Suite DPA, Google considers itself to be a data processor for the processing of 'Customer Personal Data':

*"If European Data Protection Law applies to the processing of Customer Personal Data: (...)
b. Google is a processor of that Customer Personal Data under European Data Protection Law"¹⁹⁰*

It follows from the definitions of the G Suite DPA that this data processor role is limited to the Core Services.

The G Suite DPA contains the following instructions given by the data controller (the government organisation) for the processing of personal data in Customer Data from the Core Services:

"Customer instructs Google to process Customer Personal Data only in accordance with applicable law: (a) to provide the Services and TSS; (b) as further specified via

¹⁹⁰ Google G Suite DPA, Section 5.1.1.

*Customer's and End Users' use of the Services (including the Admin Console and other functionality of the Services) and TSS; (c) as documented in the form of the applicable Agreement, including this Data Processing Amendment; and (d) as further documented in any other written instructions given by Customer and acknowledged by Google as constituting instructions for purposes of this Data Processing Amendment.*¹⁹¹

As quoted above, the G Suite DPA includes the non-limitative general purpose of 'providing the Service and TSS'. Google insists it only follows documented instructions from its customers. This purpose is not specific and explicit enough to enable government organisations to comply with their obligation to only process personal data for specific and explicit purposes.

As explained in Section 4, the G Suite DPA, public documentation, responses from Google and the technical findings from this DPIA result in the identification of 6 specific purposes for the processing of personal data in Customer Data. These purposes are however not enumerated in the G Suite DPA and therefore not part of the government organisation's documented instructions. Google seemingly considers these purposes to be compatible with the purpose of 'providing the Services and the Technical Support Services'.

Data controllers must determine the purposes of processing in a data processor agreement with the data processor. Data processors may only process personal data on behalf of the data controller.¹⁹² Therefore, Google as a data processor may not determine what purposes are compatible with the main purpose of technically delivering the G Suite service, or keeping it secure. Regardless of the contractual arrangement, if Google does determine any (compatible) purposes of processing, it acts a data controller and not as a data processor.

As detailed in Section 4.2, Google does not offer an exhaustive list of specific and explicit purposes for which Google as a data processor necessarily has to process personal data. Google only excludes a specific purpose, and promises not to process *Customer Personal Data for Advertising purposes or serve Advertising in the (Core) Services.*¹⁹³

This DPIA shows that Google factually processes personal data for purposes that are not specifically and explicitly enumerated as part of the documented instructions of the data controller. Though data processors are legally required to take adequate security measures to protect the data of all customers, such a liberty to determine purposes of the processing is not available for purposes such as scanning the contents of communications to proactively detect unlawful content. Google however, seems to deem such purposes compatible with the catch-all purpose of *providing the service*.

By determining the (compatible) purposes of processing, Google steps outside of its role as data processor. In the absence of any explicit and specific purpose in the documented instructions, Google factually acts as a data controller for personal data in Customer Data in the Core Services, but not as an independent data controller.

¹⁹¹ Clause 5.2.1 G Suite DPA.

¹⁹² Article 28(3) GDPR.

¹⁹³ Idem, Section 5.2.2, last sentence. Based on the technical research, factually Google does not seem to process the Customer Data for advertising purposes, with the exception of one bug (a DoubleClick cookie that was accidentally set through a YouTube video when logging in to the Core Service Drive). This bug shows how complicated it is, even for Google itself, to offer a tracking free version of its services.

5.2.2 *Features, and the Google Account used in conjunction with the Core Services*
During the course of this DPIA, Google explained that it processed personal data in Customer Data from the Google Account and from the Features *Spelling and Grammar, Translate and Explore* in the same way as Customer Data from the Core Services. In reply to this DPIA, Google explained that it also considers the use of Google Maps a Core Service product feature, when it is embedded in Calendar. That implies the use of this functionality is also covered by the G Suite DPA.

Google's assurances with regard to the personal data in Customer Data from the Google Account when used in conjunction with the Features need to be contractually formalised and documented. However, even if the Google Account (when used in conjunction with the Core Services) and the Features would be included under the current G Suite DPA, Google would still not qualify as a data processor. As explained above, by determining the (compatible) purposes of processing, Google steps outside of its role as data processor, and in the absence of any explicit and specific purpose in the documented instructions, Google factually acts as a data controller for personal data that falls within the scope of the G Suite DPA, but not as an independent data controller.

5.3 Data controller

Given the limitation of the scope of the G Suite DPA to personal data in Customer Data from the Core Services, and Google's explanation that this also applies to the Google Account when used in conjunction with Core Services and the Features, Google qualifies itself as a data controller for the processing of personal data in the Google Account when used outside of the Core Services, the Additional Services, Other related services such as Feedback and for all Diagnostic Data.

5.3.1 Google Account

As explained in Section 1.2, government employees must create a Google Account if they want to use the G Suite Enterprise services. When end users create their account, they have to accept the (consumer) Terms of Service and the (consumer) Privacy Policy. See [Figure 6](#).

Google distinguishes between the use of the Google Account in the Core Services, and the use of the account in other (consumer) services, as detailed in Section 1.4.2. However, this technical distinction is not yet contractually guaranteed. For end users the operational difference between the enterprise and the consumer environment may be hard to discern. This is the case, for example, when end users want to use a spellingchecker in Google Docs. If an employee uses a Chrome browser, there are three kinds of spellcheckers available, while only the Feature *Spelling and grammar* falls within the scope of the G Suite DPA.

Google qualifies itself as data controller for the Google Account that can be used for any of the 92 different consumer services.

Unless Google provides contractual assurances about the purposes for which it can process the Google Account in the Core Services, and allows admins of government organisations access to all data collected about the use of the Google Account in the Core Services, Google factually qualifies as data controller in both enterprise and consumer environments, but not as independent controller. This will be explained further in Section 5.4 below.

5.3.2 Diagnostic Data

To provide secure, well-functioning, bug free and up to date services, the processing of some Diagnostic Data about the individual use of the services may be necessary. In order to achieve such clear objectives, the data processor has a certain liberty to

decide how the personal data are processed and in which systems (with which means). However, the processor must be transparent about what personal data it needs to process, and for what purposes, in order to successfully claim to act on instructions of the controller.

In the G Suite DPA Google does not mention the Diagnostic Data at all. Diagnostic Data is therefore not covered by the G Suite DPA and Google is not a data processor when it processes Diagnostic Data.

In Section 4.2.2, ten purposes have been identified for which Google processes the Diagnostic Data relating to the use of the Core Services. These purposes have been identified in discussions with Google during the course of this DPIA.

Two of these ten identified purposes are so broad that the government organisations cannot determine what types of processing are in, or outside the scope of these purposes. These are:

- *Improving the services, based on aggregate usage information*
- *Communicating with our customers and their admins*

A third purpose, *managing G Suite accounts (including billing and financial records)*, points to Google's own legitimate business operations as (independent) controller, and can therefore not be performed at the request of a customer. Processing for Google's own legitimate business purposes should be separately defined in the contractual agreement between the Dutch government and Google.

Besides those 10 purposes, Google can potentially process these personal data for perhaps 22 different purposes in total. As it is unclear for what purposes Google processes Diagnostic Data, the government organisations that decide to use G Suite Enterprise service are not sufficiently in control.

In its opinion on the legal basis of necessity for the performance of a contract, the European Data Protection Authorities, united in the European Data Protection Board, write that data controllers of online services have a tendency to maximise the possible uses of data, without adequate specification: "*Both purpose limitation and data minimisation principles are particularly relevant in contracts for online services, which typically are not negotiated on an individual basis. Technological advancements make it possible for controllers to easily collect and process more personal data than ever before. As a result, there is an acute risk that data controllers may seek to include general processing terms in contracts in order to maximise the possible collection and uses of data, without adequately specifying those purposes or considering data minimisation obligations.*"¹⁹⁴

Similarly, the EDPB outlines the importance of separating different purposes, and warns that a generic purpose such as 'improvement' or 'developing new functions within an existing service' cannot be qualified as necessary for the performance of the contract with an end user.

While this EDPB opinion describes the legal ground that a data controller must have for the processing of the personal data of an individual customer, it is highly relevant for the relationship between data controllers and data processors as well. as it stresses that generic purposes are not acceptable and that purposes must be adequately specified.

¹⁹⁴ EDPB, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects - version adopted after public consultation, 16 October 2019, URL: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_en

Based on the arguments mentioned above, Google qualifies as data controller for the processing of Diagnostic Data about the Core Services. Google is however not an independent controller, as will be further explained in Section 5.4 below.

5.3.3

Additional Services including the Chrome OS and Chrome browser

Google qualifies itself as an independent data controller for the processing of personal data via the Additional Services, with the exception when an Additional Service is used as (part of) a *Feature* in the Core Services (as explained in Section 4.1 above).

As described in Section 3.2 of this report, the Additional Services are all turned On by default for G Suite Enterprise customers. Blocking access to these services thus requires an active intervention from admins or end user. It follows from numerous well-documented behavioural economics studies that most human behaviour is not rational, but guided by cognitive biases.¹⁹⁵ People have an irrational unwillingness to change. This '*status quo bias*' prevents people from changing the default privacy settings, even if these default settings do not match their privacy preferences. Two other cognitive biases that limit people's ability to change default privacy settings are aversion to loss (loss aversion) and a preference for the services they already have, compared to services that they do not yet use, even if that service offers more value (the endowment effect).¹⁹⁶ These cognitive limitations influence admins and end users not to make any changes to the default settings offered by Google, the more so because these choices require a deep understanding of a complex tech environment.

But even if a qualified admin were able to make a rational choice, he would lack adequate information about the kinds of personal data that Google can collect about the use of these services, and about the specific purposes for the processing of these categories of personal data. At the moment of completion of this DPIA, Google published snippets of information in many different sources. The lack of centrally accessible, limitative lists of data and purposes discourages administrators from exercising meaningful control. Since December 2020, Google publishes information for admins in its *Data Protection Implementation Guide*.¹⁹⁷

The default settings, the lack of transparency and the use of one Google Account lead to a lack of boundaries between the consumer and the enterprise environment. This may lead to a spill-over of personal data.

As explained in Section 3.1.6, if an employee is simultaneously signed in with a consumer account, Google can process the search data to enrich the Ads Personalization profile of the consumer Google Account. This spill-over may also

¹⁹⁵ Autoriteit Persoonsgegevens (Dutch DPA), Rapport definitieve bevindingen Microsoft Windows 10, De verwerking van persoonsgegevens via telemetrie, -met correcties 6 oktober 2017-, p. 135. URL: https://autoriteitpersoonsgegevens.nl/sites/default/files/01_onderzoek_microsoft_windows_10_okt_2017.pdf

¹⁹⁶ The Dutch DPA refers to Nudge and the Law: A European Perspective, red. Alberto-Alemanno, Anne-Lise Sibony, Bloomsbury Publishing, 24 September 2015, en cited research of a.o. R. Balebako, 'Nudging Users towards Privacy on Mobile Devices', CHI 2011 workshop article, A. Acquisti, Nudging Privacy. The Behavioral Economics of Personal Information (2009), IEEE Security & Privacy, and CR Sunstein, 'Deciding by Default' (2013), University of Pennsylvania Law Review. The Dutch DPA also refers to: Daniel Kahneman, Jack L. Knetsch, Richard H. Thaler, Anomalies: The Endowment Effect, Loss Aversion, and Status Quo Bias, The Journal of Economic Perspectives, 5(1), pp. 193-206, Winter 1991.

¹⁹⁷ After completion of this report, in December 2020, Google published the Google Workspace Data Protection Implementation Guide, URL https://services.google.com/fh/files/misc/google_workspace_data_protection_guide_en_dec2020.pdf

occur when a user sends Feedback from a Core Service to Google, perhaps including a screenshot or contents of a file. Or when an end user on ChromeOS must be allowed access to the Additional Service Google Play to install the Device Policy App to have the device managed by the organisation. The G Suite DPA does not apply to the use of the Google Play store, and the installation of apps via Google Play may trigger yet more data processing outside the scope of the G Suite DPA. If a Chromebook for example has installed apps from Google Play, Google explains in the Chrome Privacy Notice that Android diagnostic and usage data are sent to Google in its role as data controller. In that case Google may process these personal data for all the purposes of its (consumer) Privacy Policy.

The lack of control from government organisations over the use of the Additional Services confirms Google's own qualification as data controller, but in view of the interdependence of Core and Additional Services, not as an independent controller.

5.3.4 *Other related services*

When using the Core Services, a service may appear that can analyse and download content, such as Feedback. End users can utilise this service to upload Customer Data. That Google qualifies itself as data controller for Feedback can only be noticed by end users if they pay close attention to the hyperlinks to Google's consumer Privacy Policy and the consumer Terms of Service. See [Figure 10](#). Google has not provided a list of such services, and it is not clear why Google offers such a service as data controller while an end user is working with the Core Services.

In these circumstances, Google qualifies as controller for the personal data processing via Feedback, but not as independent controller.

5.3.5 *Technical Support data*

It is unclear whether Google processes Support Data under its (consumer) Privacy Policy or the G Suite DPA. Support Data are not covered by the definition of Customer Data under the G Suite DPA, as Customer Data are defined as data submitted, stored, sent or received via the 'Services', which do not include the Technical Support Services. As the G Suite DPA states that Google is only a data processor for the processing of personal data in Customer Data in the Core Services, Support Data would be outside the scope of the G Suite DPA. This in turn would mean Google is not a data processor, but a data controller.

However, the instructions to Google as a data processor in the G Suite DPA do include the processing of personal data in Customer Data for Technical Support Services:

*"Customer instructs Google to process Customer Personal Data only in accordance with applicable law: (a) to provide the Services and the TSS; (b) as further specified via Customer's and End Users' use of the Services (including the Admin Console and other functionality of the Services) and the TSS."*¹⁹⁸

In answer to this DPIA, Google explained: *"Google remains a data processor in respect of Customer Personal Data accessed by Support agents in order to provide support."*¹⁹⁹ T

The distinction between personal data submitted by customers' administrators (for which Google considers itself to be a data controller) and personal data in Customer Data accessed by support agents (for which Google considers itself data processor) is not clear to customers. As Google determines how, and for what purposes it may process troubleshooting and contact data, Google qualifies as data controller for the

¹⁹⁸ Google reply to part A of the DPIA.

¹⁹⁹ From responses provided by representatives of Google to SLM Microsoft Rijk during the course of the DPIA.

processing of personal data via the Technical Support Services, but not as independent controller.

5.3.6

Subprocessors

With regard to the Core G Suite Enterprise Services, Google provides a list of the subprocessors it engages.²⁰⁰ Through the G Suite DPA, customers authorise existing third party subprocessors, and generally, the engagement of new third party subprocessors.

Google will inform the Customer about a new subprocessor 30 days in advance. If the Customer wishes to object, terminating the agreement is Customer's *sole and exclusive remedy*.²⁰¹ However, the G Suite DPA contains a blanket authorisation with respect to access by Google group companies from time to time, that are not covered by the objection procedure.

[CONFIDENTIAL]

For G Suite Enterprise services, Google only uses subprocessors to provide Technical Support services. Google explains in the Google G Suite subprocessors list: *"These subprocessors have access to (a) customer information that you share explicitly in the course of a support case, including any troubleshooting material (e.g., log files, screenshots), and (b) contact, billing, and account information on file or shared with the support team. In the course of resolving a support case, only the support agents assigned to your support case will have access to project metadata and project telemetry and only while it's relevant to the troubleshooting."*²⁰²

In the underlined sentence, Google describes that its subprocessors may collect telemetry data and metadata for troubleshooting. As outlined in Section 2.2 of this report, at the time of completion of this DPIA Google provides limited and opaque information about the telemetry data it collects. Google doesn't offer any controls to influence this data processing. It follows from this lack of transparency and control that Google factually determines the scope and nature of this type of personal data processing relating to the Core Services. By doing so, it behaves as a data controller, and not as a data processor.

In reply to this DPIA, Google emphasised that subprocessors cannot access Customer Data: *"Google only uses subprocessors for Technical Support services in the G Suite Core Services, and they can only process content if an admin sends these data in a support ticket."*²⁰³ Google did not explain how subprocessors access the telemetry data.

Upon request, Google explained that it applies 4 types of security safeguards to limit subprocessor access to technical support data such as telemetry data.

- *"Subprocessors exclusively use Google-managed machines to access corporate resources*
- *Our internal systems have built in interconnected controls that will grant/ deny access to a support agent depending on systematized checks performed (i.e.: ownership of the support case)*
- *System accesses by subprocessors are systematically logged and periodically audited to ensure appropriate use*

²⁰⁰ Google G Suite subprocessors, February 2020, URL: <https://gsuite.google.com/i+ntl/en/terms/subprocessors.html>.

²⁰¹ G Suite DPA, 11.4.

²⁰² Google overview provided to SLM Microsoft Rijk of G Suite subprocessors.

²⁰³ Google response 5 June 2020.

- *Subprocessors have no access to end user Customer Data (i.e. text entered into Gmail, docs, sheets, slides, and other apps by the end user) unless this is specifically shared by the customer with the support agent during the support case.*²⁰⁴

Google explained it verifies compliance with the information security requirements through annual audits. *"This audit incorporates requirements from various sources, such as ISO 27001, SOC 2, PCI DSS, as well as the SDPA. All G Suite third-party subprocessors are in scope for an audit unless they are able to provide an unqualified independent security assessments report (ISO 27001 and SOC 2) or have recently gone through a Google Vendor Security Assessment."*²⁰⁵

Google also provided a limitative list of subprocessors who may provide support in English or Dutch to Dutch government organisations. Additionally, Google has given a presentation to the external lawyers hired by SLM Microsoft Rijk about the data processing agreements with its subprocessors. These lawyers have to assess the list of subprocessors and contents of Google's subprocessing agreements with them as part of the contractual negotiations between the Dutch government and Google upon completion of this DPIA.

For this DPIA it is relevant whether customers have meaningful control over the engagement of subprocessors by Google and the processing of their personal data by such subprocessors. Google does allow customers to object to the engagement of new subprocessors. However, customers can only object by terminating the agreement. Terminating the agreement as sole and exclusive remedy can deter data controllers from objecting to new subprocessors as the consequences of termination are far-reaching. Google therefore effectively decides which third parties engaged as new subprocessors may have access to personal data, without giving meaningful control to its customers. By doing so, Google acts as a data controller.

5.3.7 *Disclosure to law enforcement*

As mentioned in Sections 4.2 and 4.3 of this report, Google may be ordered to disclose data pursuant to requests by governmental agencies, such as law enforcement authorities. It follows from the G Suite DPA that Google will refer disclosure requests to its (Enterprise) customer, *unless the law prohibits Google from doing so on important grounds of public interest.*²⁰⁶ Google explains how it handles governmental requests for end user information: it reviews the requests, tries to narrow the request down and sometimes objects to the requests.²⁰⁷ Google also explains that it requests that the relevant authority obtains the requested data directly from the customer, (ii) reviews each request for legal validity and appropriate scope, (iii) notifies customers of a request, unless prohibited from doing so by law and (iv) provides technical tools to give customers more visibility and control on access to data. Google has opposed indefinite non-disclosure orders and filed a legal challenge in the US challenging gag orders.²⁰⁸

Google publishes statistics about these requests in semi-annual transparency reports.²⁰⁹ For the first time on 5 May 2020, Google published a separate report

²⁰⁴ Google response to this DPIA, Security safeguards third-party subprocessors.

²⁰⁵ Idem.

²⁰⁶ Google G Suite DPA.

²⁰⁷ Google, How Google handles government requests for end user information, URL: <https://policies.google.com/terms/information-requests?hl=en-GB>

²⁰⁸ Google, Advancing customer control in the cloud, URL: <https://cloud.google.com/blog/topics/inside-google-cloud/advancing-customer-control-in-the-cloud>

²⁰⁹ Google Transparency Report, Requests for end user information, URL: https://transparencyreport.google.com/user-data/overview?hl=en_GB

about requests for G Suite Enterprise accounts²¹⁰, instead of publishing combined statistics about consumer and enterprise data.

Between July 2019 and December 2019, Google received one request for disclosure of G Suite Enterprise customer information from Dutch law enforcement authorities. Overall, Google received 274 requests for G Suite Enterprise data, relating to 425 customers (domain). In 55% of the requests, Google disclosed some data. Google publishes the statistics per requesting country, not per nationality of the data subjects whose personal data are requested. Thus, these numbers do not provide insight how frequently data from Dutch customers of G Suite Enterprise have been requested by, or disclosed to, foreign governmental authorities.

In the same period Google received 486 data disclosure requests for its consumer services, relating to 723 end users/accounts from authorities in the Netherlands. Google produced data in 84% of the cases.²¹¹ Globally, for its consumer services Google received a little over 81.000 requests, relating to 175.715 end users/accounts.

Google provides an overview of requests for USA national security purposes (FISA court orders) it receives.²¹² The published number of requests is aggregated in buckets of 500 requests. Between January and December 2019, for all its worldwide (consumer and enterprise) customers, Google received between 0 and 499 requests for contact information (not content), relating to customers with an unknown residence. In that same period, Google also received between 0 and 499 requests for Customer Data relating to between 107.000 and 107.499 accounts, as well as 500 to 999 national security letters.²¹³

Google explains its procedure in its transparency reports website:

"When we receive a request from a government agency, we send an email to the end user account before disclosing information. If the account is managed by an organisation, we'll give notice to the account administrator. We won't give notice when legally prohibited under the terms of the request. We'll provide notice after a legal prohibition is lifted, such as when a statutory or court-ordered gag period has expired."²¹⁴

Google explains that it will only provide data if the requests satisfy the Global Network Initiative's Principles on Freedom of Expression and Privacy and its associated implementation guidelines.²¹⁵

According to the GDPR, only data controllers may take decisions to disclose personal data to governmental agencies outside of the EU. Article 48 of the GDPR creates an exception to this rule. This provision acknowledges that a data processor may sometimes be forced by order of a court or administrative authority in a third country, outside of the EU, to transfer or disclose personal data. Such orders may

²¹⁰ Google, Enterprise Cloud requests for customer information, URL: <https://transparencyreport.google.com/user-data/enterprise>

²¹¹ Google Transparency Report Netherlands, https://transparencyreport.google.com/user-data/overview?hl=en&user_data_produced=authority:NL;series:compliance&lu=legal_process_breakdown&user_requests_report_period=series:requests,accounts;authority:NL;time:&legal_process_breakdown=expanded:0

²¹² Google, United States national security requests, URL: https://transparencyreport.google.com/user-data/us-national-security?hl=en_GB

²¹³ Google, United States national security requests, URL: https://transparencyreport.google.com/user-data/us-national-security?hl=en_GB

²¹⁴ Idem.

²¹⁵ Global Network Initiative, the GNI Principles, URL: <https://globalnetworkinitiative.org/gni-principles/>

only be recognised or enforced in any manner if they are based on an international agreement such as a mutual legal assistance treaty. This exception is titled “*Transfers or disclosures not authorised by Union law*”. This exception however does not change the main rule that only data controllers may take decisions whether to hand over personal data to governmental agencies outside of the EU. That is why data processor must redirect such orders to the data controllers.

Only a data controller can decide about an important purpose of the processing as disclosure to governmental agencies outside of the EU, Google acts as a data controller when hands over personal data (be it Customer Data, Account Data or Diagnostic Data) to a law enforcement authority, security agency or secret service in the USA, when Google is not allowed to redirect the order to its customer. This separation of Google’s role as data processor or data controller is not yet contractually guaranteed.

5.4 Joint controllers

Government organisations that use G Suite Enterprise software have a legitimate expectation that Google solely acts as a data processor for the personal data that Google processes through and about the use of G Suite Enterprise. However, in practice they enable Google to collect and process various personal data as a data controller for Google’s own purposes.

As outlined in Sections 5.2 and 5.3.1 to 5.3.7 above, Google qualifies as a data controller for:

1. The Customer Data in the Core Services and content data in the Additional Services;
2. the Google Account (both when used in the Core Services and in the Additional Services);
3. the Diagnostic Data of the Core Services and the Additional Services;
4. personal data processed through Feedback;
5. some of the Support Data (not being personal data in Customer Data);
6. the engagement of new subprocessors; and
7. the disclosure of personal data to law enforcement, security agencies, and secret services in case Google is prohibited from redirecting the authorities to the customer.

However, Google cannot be qualified as an independent data controller for the processing with respect to the personal data listed in 1 to 7 above.

According to three judgments of the European Court of Justice parties can factually become joint controllers.²¹⁶ That is even the case if the roles are unevenly distributed, or if the customer does not have access to the personal data processed by the supplier of the service. This can be the case if (i) the supplier processes the data for its own purposes, and (ii) this processing can only be performed (inextricable link) because the customer enables this data processing by selecting this supplier.

This enabling of processing by the supplier is clearly the case for the Google Account Data, the Diagnostic Data (including the website and telemetry data) and the Support Data. By engaging Google as a data processor for G Suite Enterprise,

²¹⁶ European Court of Justice, C-40/17, 29 July 2019, Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV, ECLI:EU:C:2019:629, C210/16, 5 June 2018, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein versus Wirtschaftsakademie Schleswig-Holstein GmbH, ECLI:EU:C:2018:388. See in particular par. 38-43. Also see: C-25/17, 10 July 2018, Tietosuojavaltutettu versus Jehovah’s Witnesses — Religious Community, ECLI:EU:C:2018:551, par. 66-69.

government organisations enable Google to collect personal data that Google otherwise would not be able to process.

Google operates under the incorrect assumption that it has the discretion to process personal data obtained through use of G Suite Enterprise as an independent data controller for purposes that have not been authorised by the government organisation. Google does so by simply referring to its (consumer) Privacy Policy and limiting all data protection guarantees to the personal data in Customer Data. This is wrong. As enumerated in Section 4.3, in its role as data controller Google contractually permits itself to process personal data for at least 33 purposes. Many of these of purposes are not specific or explicit.

If Google wants to offer functionality or process personal data that are strongly linked to the use of G Suite Enterprise as independent data controller, such processing and such functionalities should be disabled by default. The controls to enable these services and functionalities should be accompanied with very clear information what the data protection consequences are when end users and admins opt-in to such functionality. In all circumstances, Google should offer controls for admins to permanently block such processing and functionalities for all end users. Without such measures and controls, there are no clear boundaries between the data processor and the data controller domains.

There is an inextricable link between (i) the use of G Suite Enterprise to create, store, send and seek information, and (ii) the collection of Diagnostic Data by Google about the use of G Suite Enterprise. Clearly, Google cannot collect any Diagnostic Data about Core Services if end users do not use such Core Services. There is a similar inextricable link for the Google Account Data, as the use of the Google Account is mandatory for employees of Dutch government organisations that decide to use G Suite Enterprise. There is only one Google Account for both consumer and enterprise environments, and Google does not yet offer contractual guarantees that it only processes the Google Account as data processor when used inside of the Core Services. Therefore, Google's role as data processor cannot (yet) be distinguished from its role as data controller.

The Additional Services and Other related services such as Feedback and Chrome's *Enhanced Spellchecker*, as well as Ads Personalization are enabled by default for customers outside the education sector, as well as Ads Personalization. As described in Section 3.2.4 of this report, government administrators have no central controls to minimise the collection of Diagnostic Data (including telemetry and website data), cannot centrally block or limit the collection by Google of telemetry data or centrally disable Ads Personalization. These data include personal data such as the local IP address, what apps are used and when, Bluetooth use including the hashed MAC addresses, when biometric authentication is used and the occurrence (not contents) of crashes. As a result the customers of G Suite Enterprise become joint controllers with Google for the resulting data processing by Google outside of its data processor role.

If government organisations do not actively disable the default transfer of location data from the Chrome browser on Android mobile devices to Google Search (as explained in Section 3.2.2), they also become joint controllers for the collection of personal data for general analytic purposes and for personalised advertising aimed at the end user.

In sum, as long as the government organisations are not in a position to determine and exclude the above purposes of the processing, while Google can only collect these personal data in its role as data processor, in practice they become joint controller for these data processing operations with Google.

As explained in Sections 4.2 and 4.3 above, Google reserves the right as (joint) data controller to process the personal data for at least 33 purposes set out in its (consumer) Privacy Policy, plus additional specific purposes for the Chrome browser. As a result of being joint controllers, the government organisations can be held accountable for the processing of personal data relating to all kinds of data subjects for these purposes.

The only exceptions, where Google may act as independent controller, are the processing -when proportionate - for Google's own legitimate business purposes (e.g. invoicing) and disclosures to authorities, but only if Google was legally prohibited from forwarding the request or order to the customer.

6. Interests in the data processing

This section outlines the different interests of Google and Dutch government organisations in the use of G Suite Enterprise. The interests of the Dutch government organisations may align with the interests of their employees, but this is not always the case. This section does not include an analysis of the fundamental data protection rights and interests of employees as data subjects. How their rights relate to the interests of Google and the Dutch government organisations is analysed in part B of this DPIA.

6.1 Interests of the Dutch government organisations

Dutch government organisations have security, efficiency and compliance reasons to use cloud productivity software such as G Suite Enterprise.

The G Suite Enterprise services offer functionality that allow end users to jointly and simultaneously access and work on files and documents that are stored in Google's cloud. The use of a cloud environment makes it easier for end users to share information with each other instead of distributing copies, such as attachments to an email. Similarly, file sharing is easier and safer with Drive. Many organisations still share files via network drives for document storage or via local storage servers. In practice, employees increasingly share information via consumer versions of cloud products because existing solutions with network drives and local storage are not sufficient. Many people use, for example, Dropbox or WeTransfer to share files. This can result in a parallel network that the government organisations cannot manage.

It is a well-known IT problem to properly organise and manage the access authorisations for the network drives. If end users have access to documentation to which they should not have access based on their role, this results in multiple security and privacy risks. In contrast to the network drives, Google offers transparency and controls about the rights that have been granted for access to the information with a number of features such as the Google Drive Access checker, Data Loss Prevention, Access Transparency, G Suite Security Center, Admin Audit and Reports, and Shared Drives. These tools also allow end users or admins, depending on the application, to see who has access to what information.

Government organisations also have a strong interest in providing reliable, always working, well integrated and location independent productivity tools to their employees. Well-functioning for the Dutch government also means that the software has to be accessible on different kinds of devices, and from different locations. The ability for employees to seamlessly work at home through for example collaboration tools like Google+, Groups for Business and Hangout, is more urgent than ever since the outbreak of the COVID-19 pandemic.

The use of the webbased G Suite services may allow government organisations to cut back spending on the maintenance of desktops in offices, and potentially switch to the use of Chromebooks. Because G Suite is widely used by consumers, government employees may also require less IT support because they are already accustomed with the G Suite services

Additionally, the ability to access log data about end user behaviour through the many different audit logs in G Suite Enterprise is essential for government organisations to comply with their own obligations as data controllers to detect security incidents. By using log files such as the Drive and the Login audit logs the administrators can access data about end users' sign-in attempts and access to personal data in files stored in Drive. This information is necessary to detect and mitigate possible security incidents and data breaches.

Furthermore, G Suite Enterprise enables administrators to encrypt information on end-user devices. Especially on mobile devices, such encryption is required to minimise the risks of data breaches.

In contrast with the above-mentioned interests in the use of cloud providers, Dutch government organisations have a security and geopolitical interest in storing data in local data centres or, alternatively, in a limited number of data centres in the EU. The Ministry of Defence even has a military state sovereignty interest to only store data in a sovereign cloud.

6.2 Interests of Google

Google has a strong financial and economic interest in selling customers a monthly cloud-based subscription service in order to increase its revenue.

Google also has an interest in using the data it collects or otherwise obtains through the provision of the G Suite services for many different purposes. Many of the 33 purposes in Google's (consumer) Privacy Policy represent Google's interest in using data, for example 'Develop new products and features' (purpose 5), 'Use cookies for many purposes' (purpose 29) and 'Performing research'.

Google has a business and marketing interest in differentiating between its consumer advertising revenue-based business model, and its corporate cloud subscription-based business model. In Google's Cloud Privacy Principles²¹⁷, Google promises, amongst others, not to process Customer Data for advertising, and to allow customers to control what happens with their data.

Google competes with Microsoft, that has similar offerings for consumer and business productivity software. Google has business and economic interests in continuing to improve and develop its services and products to stay competitive.

As a cloud provider, Google has a strong interest in promoting the security of its services to convince potential customers of the reliability and impenetrability of its services. Google writes: "*Google employs more than 500 full-time security and privacy professionals, who are part of our software engineering and operations division. Our team includes some of the world's foremost experts in information, application and network security.*"²¹⁸ Google also writes that this "security team

²¹⁷ Google, Privacy, Google Cloud Trust Principles, URL:

<https://cloud.google.com/security/privacy>

²¹⁸ Google, Google Cloud Security and Compliance, URL:

<https://gsuite.google.com/learn-more/security/security-whitepaper/page-2.html>

actively scans for security threats using commercial and custom tools, penetration tests, quality assurance (QA) measures and software security reviews.”²¹⁹

Google has a commercial interest in attracting customers at a young age. The longer a user uses the same e-mail address, the higher the switching costs. The UK supervisory authority Ofcom for example has warned British telecom providers that most people are being put off switching providers to get better deals, because of the hassle of losing their email addresses.²²⁰ Google attracts end users in the Netherlands at a very young age. According to the central IT support and procurement organisation for primary and secondary schools in the Netherlands, Kennisnet, Google has a market share of 70% with the ‘free’ services G Suite for Education.²²¹ This means children become accustomed to a ‘free’ Gmail address at a very young age, which they may likely to keep on using when they grow up.

Google has a clear financial, business and economic interest in certain default settings. Google explained that all Additional Services are turned on *by design*. Some Additional Services contain and generate personalised advertising. As one of the world’s biggest ad networks, Google has a strong financial interest in the delivery of ads, in particular targeted ads. Google believes that by showing personalised ads it is delivering value to online end users, since they do not have to pay with money for many services.²²² In 2019, Google gained a revenue of approx. 134 billion US dollar with its advertising business.²²³ In 2019, Google cloud revenues amounted to only 5.5% of its global revenues.²²⁴ These cloud revenues consist primarily of revenues from Google Cloud Platform (GCP). This includes infrastructure, data and analytics, and other services such as G Suite and other enterprise cloud services.²²⁵

6.3 Joint interests

The interests of Google and the Dutch government align when it comes to the use of data for security purposes. An example is the use of Diagnostic Data to protect personal data stored in, or generated by the use of, the G Suite services against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access, and by restoring timely access to personal data following an incident.

²¹⁹ Idem.

²²⁰ BBC News, 22 February 2020, Email address charges branded ‘daylight robbery’, URL: <https://www.bbc.com/news/business-51571275>

²²¹ Item in Dutch national newspaper De Volkskrant, Google wordt steeds grotere speler op scholen, tot zorg van privacyorganisaties, 1 november 2019, URL: <https://www.volkskrant.nl/nieuws-achtergrond/google-wordt-steeds-grotere-speler-op-scholen-tot-zorg-van-privacyorganisaties~bae18dcd/>

²²² See for example Google, Our Privacy and Security Principles, URL: <https://safety.google/principles/> “We also use data to serve more relevant ads. While these ads help fund our services and make them free for everyone, it’s important to clarify that our users’ personal information is simply not for sale.” Or Understanding how Google ads work, URL: <https://safety.google/privacy/ads-and-data/> “We use data to make our services more useful and to show relevant advertising, which helps make our services free for everyone.”

²²³ Statista, Annual revenue of Google from 2002 to 2019, 5 February 2020, URL: <https://www.statista.com/statistics/266206/googles-annual-global-revenue/> In the most recently reported fiscal year, Google’s revenue amounted to 160.74 billion US dollars. Google’s revenue is largely made up by advertising revenue, which amounted to 134.81 billion US dollars in 2019. See also Alphabets 10K filing at the US Security and Exchange Commission over 2019, URL: https://www.sec.gov/cgi-bin/viewer?action=view&cik=1652044&accession_number=0001652044-20-000008&xbrl_type=v. According to this filing, the revenue was 161.857 billion USD.

²²⁴ Idem, Distribution of Google segment revenues from 2017 to 2019, URL: <https://www.statista.com/statistics/1093781/distribution-of-googles-revenues-by-segment/>

²²⁵ Ibid.

Google's interest in developing new services and improving or expanding functionalities can also be aligned with the interests of the Dutch government organisations, provided that such new services or improvements follow the restrictions set by administrators, and are not activated by default. Similarly, Google and government organisation's interests may be aligned in the processing of some personal data by Google to deliver well-functioning (bug free) services, to prevent loss of labour capacity for the Dutch government.

In sum, Google has financial, economic and commercial/business interests to provide secure and innovative services. Google also has strong commercial/business interests in default settings that allow frictionless use of its Additional Services and that maximise the collection of Diagnostic Data. Some interests are consistent with the Dutch government's interests, but others are not.

7. Transfer of personal data outside of the EEA

The GDPR contains specific rules for the transfer of personal data to countries outside the European Economic Area (EEA).²²⁶ In principle, personal data may only be transferred to countries outside the EEA if the country has an adequate level of protection. That level can be determined in a number of ways.

The European Commission can take a so-called adequacy decision. This means that the country in question has a level of protection comparable to that applied within the EEA. Currently, the European Commission made adequacy decisions with respect to Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the United States of America (limited to the Privacy Shield framework) as providing adequate protection.

The Privacy Shield framework is an agreement between the EU and the USA about the level of protection of personal data. Via the EU-U.S. Privacy Shield framework (formerly: Safe Harbour), US companies can self-certify as to their standard of protection of personal data. Notwithstanding other requirements under the GDPR, personal data can be transferred to Privacy Shield certified companies without any further safeguards.

Personal data may also be transferred from the EEA to third countries outside of the EEA using Standard Contractual Clauses (SCC, also known as EU model clauses) adopted by the European Commission on the basis of the (previous) Data Protection Directive. These clauses (hereinafter: SCC) contractually ensure a high level of protection.

At the time this DPIA was written, Google used a combination of two measures: the SCC and the Privacy Shield.²²⁷ Google has since switched to only use SCCs for the transfer. G Suite Enterprise customers in the EU can accept the SCC as a transfer

²²⁶ Articles 44 to 49 GDPR.

²²⁷ Google writes in a blog that its model clauses were approved by the data protection authorities in the EU, in December 2016. The approval decision can be found at: https://cloud.google.com/files/2016-12-30_Common_Opinion_for_G-Suite.pdf Google blog URL: <https://www.blog.google/products/google-cloud/eu-data-protection-authorities-confirm-compliance-google-cloud-commitments-international-data-flows/>

instrument for personal data in Customer Data from Core Services.²²⁸ This choice is not available for personal data in Additional Services, Support Data and for Diagnostic Data. The transfer of those personal data from customers in the Netherlands to Google’s cloud servers in the USA takes place on the basis of the EU-U.S. Privacy Shield. Google has self-certified itself under this instrument.²²⁹

Although both transfer instruments are legally valid, and have been approved by the European Commission, there are doubts about the future validity of these instruments for transfer to the US. Both instruments are the subject of proceedings before the European Court of Justice. On 16 July 2020 the Court is expected to rule whether these agreements offer sufficient protection against the risks of interception of data in transit and mass surveillance in the United States. These risks have been revealed by whistle blower Edward Snowden.²³⁰

In response to a question about Google’s preparations for this ruling, Google has indicated it can quickly adopt updated transfer mechanisms when offered by the European Commission, if both the Privacy Shield and the SCC were invalidated simultaneously or in short order.²³¹

Figure 32:²³² Google table data region selection

Which services and data are covered by a data region policy?

Primary data

Data region policies cover the primary data-at-rest (including backups) for these G Suite Core Services:

G Suite Core Service	Covered data
Calendar	Event titles, descriptions, dates, times, frequencies, invitees, locations
Drive	Original file content uploaded to Drive
Forms	Text, embedded images, responses
Gmail	Subjects, bodies, attachments, senders, message recipients
Google Docs, Sheets, Slides	File body text, embedded images, embedded drawings, associated end user-generated comments
Google Chat	Messages, attachments
Keep	Note text and title, images, drawings and audio recordings
New Sites	Text, embedded images, embedded site information, embedded HTML/CSS/Javascript
Vault	Exports

For data region settings, the Drive Enterprise edition supports Drive, Docs, Sheets, Slides, and Vault only.

²²⁸ As well as services identified as ‘Other Services’ in the G Suite Services Summary and services described in the Complementary Product Services provided under a separate agreement. These services are out of scope of this DPIA.

²²⁹ Google LLC has self-certified its compliance on 22 September 2016 and is an active participant since. See: <https://www.privacyshield.gov/participant?id=a2zt000000001L5AAI>

²³⁰ After completion of this DPIA, the European Court of Justice has ruled in Case C 311/18 on the transfer from Facebook Ireland to Facebook Inc. in the US on the basis of the Standard Contractual Clauses. The Court declared the Privacy Shield invalid. Since, the European Commission and the European Data Protection Authorities have been working on guidance and new Standard Contractual Clauses to legitimise the ongoing transfer of personal data from the EU to the USA in the absence of an adequacy agreement.

²³¹ From responses provided by representatives of Google to SLM Microsoft Rijk during the course of this DPIA

²³² Google, What data is covered by a data region policy?, URL: <https://support.google.com/a/answer/9223653?hl=en> The information on this page is dynamic. This version was captured on 16 June 2020.

In G Suite Enterprise, Google allows customers to choose between storage in datacentres in the EU or in the USA with respect to Customer Data, from some Core Services. As shown in [Figure 32](#) above, this choice covers Customer Data actively inputted in Calendar, Drive, Forms, Gmail, Google Docs, Sheets, Slides, Hangouts Chat, Keep, New Sites and Vault.²³³ This data region choice also applies to the backups.²³⁴

All other personal data, such as Diagnostic Data (including website and telemetry data) and authentication data relating to the Google Account may be processed in any of Google's global data centres. Google explains on its site about its datacentres: *"Rather than storing each user's data on a single machine or set of machines, we distribute all data — including our own — across many computers in different locations. We then chunk and replicate the data over multiple systems to avoid a single point of failure. We name these data chunks randomly, as an extra measure of security, making them unreadable to the human eye."*²³⁵

Google currently has 21 datacentres in total, of which five are located in Europe: in Dublin (Ireland), Eemshaven (Netherlands), Frederician (Denmark), Hamina (Finland) and St. Ghislaine (Belgium).²³⁶

Figure 33: Google map with datacentres



Contractually Google only applies the G Suite DPA to Customer Data of the Core Services. The Customer Data can be routed via other locations during the transfer and can also be processed in other regions. However, Google encrypts all transit traffic data, and all data at rest.²³⁷ Technically, the routing of packets via the Internet works in such a way that the paths (and therefore locations) that will be followed cannot be determined in advance.

²³³ Google, What data is covered by a data retention policy?, URL: <https://support.google.com/a/answer/9223653?hl=en>

²³⁴ Idem.

²³⁵ Google datacenters, We safeguard your data, URL: <https://www.google.com/about/datacenters/locations/>

²³⁶ Ibid.

²³⁷ Google writes: *"We automatically encrypt your data both in transit outside of physical boundaries not controlled by Google and at rest by default and provide numerous ways for you to control your own encryption keys and data access."* URL: <https://cloud.google.com/security/compliance/government-public-sector>

Google may be ordered by U.S. courts to grant law enforcement access to data stored in data centres in the EU. The U.S. CLOUD Act extends the jurisdiction of North American courts to all data under the control of U.S. companies, even if those data are stored in data centres outside the territory of the United States.

As explained by the EDPB and the European Data Protection Supervisor (EDPS) in their opinion on the CLOUD Act to the LIBE Committee of the European Parliament, transfers of personal data from the EU must comply with the Articles 6 (lawfulness of processing) and 49 (derogations for specific situations) of the GDPR. In case of an order based on the US CLOUD Act, the disclosure and transfer can only be valid if recognised by an international agreement between the EU and the USA.

The EDPB and EDPS write: "*Unless a US CLOUD Act warrant is recognised or made enforceable on the basis of an international agreement, and therefore can be recognised as a legal obligation, as per Article 6(1)(c) GDPR, the lawfulness of such processing cannot be ascertained, without prejudice to exceptional circumstances where processing is necessary in order to protect the vital interests of the data subject on the basis of Article 6(1)(d) read in conjunction with Article 49(1)(f).*"²³⁸

In their cover letter, the data protection authorities "*emphasise the urgent need for a new generation of MLATs to be implemented, allowing for a much faster and secure processing of requests in practice. In order to provide a much better level of data protection, such updated MLATs should contain relevant and strong data protection safeguards such as, for example, guarantees based on the principles of proportionality and data minimisation.*"²³⁹ Additionally, the EDPB and the EDPS refer to the ongoing negotiations about an international agreement between the EU and the US on cross-border access to electronic evidence for judicial cooperation in criminal matters and negotiating directives.²⁴⁰

In the G Suite DPA, Google contractually commits to maintaining certificates for ISO 27001, ISO 27017 and ISO 27018. Google will also produce SOC 2/3 audit reports during the term of the agreement.²⁴¹ The 2018 SOC 3 report is publicly available without non-disclosure agreement.²⁴² Google explains that this audit is not aimed at privacy, but at compliance with security principles.²⁴³

8. Techniques and methods of the data processing

As explained in Section 2 of this report, Google collects personal data in multiple ways. Google collects Customer Data and Support Data when they are submitted or sent by or on behalf of customers. In addition, Google collects Diagnostic Data about the use of its Core Services, the Additional Services, the Google Account and Other related services such as Feedback.

²³⁸ Annex EDPB and EDPS joint response to US CLOUD Act, 10 July 2019, p. 8.

URL: https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_en.

²³⁹ Idem, cover letter.

²⁴⁰ Council Decision authorising the opening of negotiations, 6 June 2019, URL: <https://data.consilium.europa.eu/doc/document/ST-10128-2019-INIT/en/pdf> and; <https://data.consilium.europa.eu/doc/document/ST-10128-2019-ADD-1/en/pdf>.

²⁴¹ Also see Google Cloud Security and Compliance, URL: <https://gsuite.google.com/learn-more/security/security-whitepaper/page-8.html>.

²⁴² SOC 3 report for the Period 1 May 2017 to 30 April 2018, URL:

https://services.google.com/fh/files/misc/spr_2018_g_suite_soc3_report.pdf

²⁴³ Google Cloud Security and Compliance, URL: <https://gsuite.google.com/learn-more/security/security-whitepaper/page-5.html#soc>

As described in Section 2 of this report, Diagnostic Data collected by Google may contain content from files and messages that were obtained by Google as Customer Data in the following ways:

- the Drive audit log includes file and path names of documents (*Item name*);
- words and sentences from documents may be collected in Diagnostic Data about the use of the Feature *Spelling and Grammar*;
- telemetry data from *Enhanced Spellingchecker* in the Chrome browser may include content from files; and
- content may be included in crash reports sent by telemetry clients in the Chrome browser and installed G Suite Core Services apps.

Although Google does not provide information about, or access to, the Diagnostic Data from its Additional Services, it is likely that Google generates the same kind of Diagnostic Data on its cloud servers as it generates about the Core Services, as shown in the audit logs. That means that Google is likely to process file and path names and subject lines in Diagnostic Data when an end user uses an Additional Service such as Google Groups, Classroom, Photos or sets keywords in Google Alerts.

For the avoidance of doubt, the Diagnostic Data streams mentioned above are separate from, and in addition to, Customer Data that end users provide to Google.

8.1 Anonymisation

According to the guidance from the Data Protection Authorities in the EU, anonymisation is a complex and dynamic form of data processing.²⁴⁴ Often, organisations still possess original data, or continue to collect pseudonymised data.

As long as there is a realistic possibility to re-identify individuals based on data that are masked, scrubbed from obvious identifiers or otherwise de-identified, such data cannot be considered anonymous and the organisation must still comply with all GDPR requirements with regard to the processing of personal data. Furthermore, the process of anonymization constitutes processing of personal data and is therefore subject to the GDPR.

Google provides a public explanation of two of its anonymisation techniques.²⁴⁵

As quoted in Section 1.4.3 of this report, Google applies anonymisation to Diagnostic Data and Customer Data when an Additional Service is included as a 'Feature' of a Core Service, such as the use of Maps and Translate. Google did not provide specific information about the anonymisation techniques it applies in this case, and did not show any examples to the researchers. Google provided a general explanation what key techniques it may use to anonymise data.

[CONFIDENTIAL]

Key techniques used by Google to anonymize data include:

- *the computation of aggregate values across a population, or the grouping of individuals such that values are shared;*
- *sampling: the computation of aggregate data based on a sample that includes a small portion of the overall population*

²⁴⁴ Anonymisation Guidelines from the Article 29 Working Party, WP216, Opinion 05-2014 on Anonymisation Techniques, URL: http://ec.europa.eu/justice/Article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

²⁴⁵ Google, How google anonymizes data, URL: <https://policies.google.com/technologies/anonymization>

- *generalizing the data (see WP216, p. 12 and 16): there are certain data elements that are more easily connected to certain individuals. In order to protect those individuals, Google uses generalization to remove a portion of the data or replace some part of it with a common value. For example, Google may use generalization to replace segments of all area codes or phone numbers with the same sequence of numbers; and adding noise to data (see WP216, p. 12):*
- *differential privacy (see WP216, p. 15) describes a technique for adding mathematical noise to data. With differential privacy, it is difficult to ascertain whether any one individual is part of a data set because the output of a given algorithm will appear the same, regardless of whether any one individual's information is included or omitted.*

In most circumstances Google will implement a combination of these techniques to effectively anonymize identifiable end user data.

In any case, there is no single method of anonymisation that is effective under all circumstances. When anonymizing data, Google will assess the circumstances on a case-by-case basis (see WP216 p. 24) and develop a method of anonymisation such that the data cannot be attributed, directly or indirectly, to an individual, including consideration of the following factors:

- *the purpose of anonymizing the data and how the data will be used after it has been anonymised (see WP216 p. 23); who will have access to the data after it has been anonymised; what, if any, limitations or controls on re-identification apply to the intended audience; what other information, tools, or resources are available to those parties that may enable reidentification;*
- *how this information will be made available, e.g. whether access will be granted to the whole data set in fixed form, or whether the audience will be able to query the data set interactively;*
- *how likely, difficult, or possible it may be to re-identify the data based on the available data and resources;*
- *the sensitivity of the underlying data, the potential for harm to the data subjects, and the extent to which there may be a motive to re-identify the data; and*
- *the impact that releasing the data may have on the anonymisation of other available collections of data.*

In accordance with recital 26 of the GDPR, personal data that has undergone pseudonymisation as defined in Art. 4 (5) GDPR, i.e. it can still be attributed to a natural person by the use of additional information kept separately by the controller, is considered by Google to still be information on an identifiable natural person, i.e. personal data (also see WP216, p. 10) ²⁴⁶

In the context of this DPIA, Google has provided information about its anonymization processes that it has requested to remain confidential. Google has not provided access to any data collected in the context of this DPIA that it considered anonymised. This means Google's assurances could not be verified.

The removal (erasure or deletion) of personal data after its collection also constitutes processing of personal data subject to the GDPR. The fact that Google deletes certain personal data from the log files and applies different anonymisation techniques, makes no difference to the assessment that Google processes personal data via these log files.

²⁴⁶. From responses provided by representatives of Google to SLM Microsoft Rijk during the course of the DPIA.

9. Additional legal obligations: e-Privacy Directive

This section only describes the additional obligations arising from the current ePrivacy Directive and (possible) future e-Privacy Regulation. In view of the limited scope of this DPIA, other legal obligations or frameworks (for example in the area of information security, such as BIO) are not included in this report.

Certain rules from the current ePrivacy Directive apply to the storage of information on, and retrieval of that stored information from, browsers with pixels and cookies and similar technologies such as tracking pixels. These rules also apply to software installed on devices that sends information via the Internet through an inbuilt telemetry client. Article 5(3) of the ePrivacy Directive was transposed in Article 11.7a of the Dutch Telecommunications Act. Consent is required prior to the retrieval or storage of information on the devices or browsers of end users, unless one of the exceptions applies, such as the necessity to deliver a requested service, or necessity for the technical transmission of information. The same consent requirement applies to the capturing of information about the use of the installed G Suite iOS and Android apps that send information over the Internet.

The consequences of this provision are far-reaching, as it requires clear and complete information to be provided to the end user prior to data processing. Part B of this DPIA discusses the (im)possibility of obtaining valid end user consent for the processing of Diagnostic Data from the different services that are part of, or can be used in conjunction with, G Suite Enterprise.

The current ePrivacy Directive (as transposed in the Netherlands in Section 11 of the Telecommunications Act) also includes rules on the confidentiality of data from the content and on communication behaviour. Article 5(1) obliges Member States to guarantee the confidentiality of communications and related traffic data via public communications networks and publicly available electronic communications services. Article 6(1) obliges providers of publicly available telecommunications services to erase or make the traffic data anonymous as soon as they are no longer needed for the purpose of the transmission of the communication.

Although the confidentiality rules in the current ePrivacy Directive do not apply to providers of software in the cloud (even though this always involves communication via a public electronic communications network), the future ePrivacy Regulation will make these rules applicable to Google as a provider of email, chat and voice services.²⁴⁷

On 10 January 2017, the European Commission published a proposal for a new ePrivacy Regulation.²⁴⁸ The proposed Article 8(1), *Protection of information stored in terminal equipment of end users and related to or processed by or emitted by equipment*, extends the current consent requirement for cookies and similar

²⁴⁷ See recital 22 in the ePrivacy directive 2002/58/EG, revised in 2009 by the Citizens' Rights Directive 2009/136/EG: "*The prohibition of storage of communications and the related traffic data by persons other than the end users or without their consent is not intended to prohibit any automatic, intermediate and transient storage of this information in so far as this takes place for the sole purpose of carrying out the transmission in the electronic communications network and provided that the information is not stored for any period longer than is necessary for the transmission and for traffic management purposes, and that during the period of storage the confidentiality remains guaranteed.*"

²⁴⁸ European Commission, Proposal for a Regulation on Privacy and Electronic Communications, 10.1.2017 COM(2017) 10 final, URL: <https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation>

techniques to the use of all processing and storage capabilities of terminal equipment.

The European Parliament adopted its position on 23 October 2017. It added a specific exception for updates and in relation to employees. The EP proposes to add two new exceptions to the consent requirement in Article 8(1), namely if it is necessary for security updates and for the performance of work by employees.

it is necessary to ensure security, confidentiality, integrity, availability and authenticity of the terminal equipment of the end-user, by means of updates, for the duration necessary for that purpose, provided that:

- (i) this does not in any way change the functionality of the hardware or software or the privacy settings chosen by the end user;*
- (ii) the end user is informed in advance each time an update is being installed; and*
- (iii) the end user has the possibility to postpone or turn off the automatic installation of these updates;*

The EP also proposed:

in the context of employment relationships, it is strictly technically necessary for the execution of an employee's task, where:

- (i) the employer provides and/or is the end user of the terminal equipment;*
- (ii) the employee is the end user of the terminal equipment; and*
- (iii) it is not further used for monitoring the employee.*

The Council of Ministers has been debating the e-Privacy Regulation for two and a half years, since October 2017. The most recent complete text dates from 6 March 2020.²⁴⁹ The Croatian Presidency of the EU recently announced it will transfer further work on the Regulation to the German Presidency (starting 1 July 2020).²⁵⁰

In a first complete concept, published on 19 October 2018, the Council proposed to follow Parliament's line with regard to employees and security updates. The representatives of the Member States also wanted to allow employers to base processing operations on employees' consent, without any reflection on the conflict with the legal presumption in Article 7(4) and recital 43 of the GDPR that consent cannot be given freely if there is a clear power imbalance between the data subject and the data controller.

The Council's proposal for Article 8 of the ePrivacy Regulation was significantly amended since February 2020, by introducing a general legitimate interest ground. The Council proposes to rename Article 8: *Protection of end users' terminal equipment information*.

(Art 8 (1) The use of processing and storage capabilities of terminal equipment and the collection of information from end users' terminal equipment, including about its software and hardware, other than by the end-user concerned shall be prohibited, except on the following grounds:

(...)

²⁴⁹ Council of the European Union, Interinstitutional file 2017/0003 (COD), Brussels 17 October 2019, 13080/19 URL: https://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=consil:ST_14447_2019_INIT . For an overview of the earlier proposed versions of the regulation by the council, see: https://eur-lex.europa.eu/procedure/EN/2017_3#2019-11-08_DIS_byCONSIL .

²⁵⁰ Council of the European Union, Progress Report 3 June 2020, URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_8204_2020_COR_1&from=EN . "The Croatian Presidency is therefore committed to work closely with the incoming German Presidency in June to facilitate further discussions and to ensure smooth progress on the file."

(c) it is necessary for providing a service requested by the end-user;
~~*(da): it is necessary to maintain or restore the security of information society services, prevent fraud or detect technical faults for the duration necessary for that purpose;*~~
or
~~*(e) it is necessary for a software update provided that:*~~
~~*(i) such update is necessary for security reasons and does not in any way change the privacy settings chosen by the end-user,*~~
~~*(ii) the end-user is informed in advance each time an update is being installed, and*~~
~~*(iii) the end-user is given the possibility to postpone or turn off the automatic installation of these updates;*~~
~~*or*~~
(g) it is necessary for the purpose of the legitimate interests pursued by a service provider to use processing and storage capabilities of terminal equipment or to collect information from an end-user's terminal equipment, except when such interest is overridden by the interests or fundamental rights and freedoms of the end-user. The end-user's interests shall be deemed to override the interests of the service provider where the end-user is a child or where the service provider processes, stores or collects the information to determine the nature and characteristics of the end-user or to build an individual profile of the end-user or the processing, storage or collection of the information by the service provider contains special categories of personal data as referred to in Article 9(1) of Regulation (EU) 2016/679.²⁵¹

The Council explains in the new recital 21b:

A legitimate interest could be relied upon where the end-user could reasonably expect such storage, processing or collection of information in or from her or his terminal equipment in the context of an existing customer relationship with the service provider.
For instance, maintaining or restoring the security of information society services or of the end-user's terminal equipment, or preventing fraud or detecting technical faults might constitute a legitimate interest of the service provider.
Similarly, using the processing storage capabilities of terminal equipment is to fix security vulnerabilities and other security bugs, provided that such updates do not in any way change the functionality of the hardware or software or the privacy settings chosen by the end-user and the end-user has the possibility to postpone or turn off the automatic installation of such updates. Software updates that do not exclusively have a security purpose, for example those intended to add new features to an application or improve its performance, should not be considered as a legitimate interest.

The Council proposes to add an exception for security purposes to Article 6, with rules on the processing of electronic communications data (both content and traffic data)

²⁵¹ Idem.

Article 6

1. Providers of electronic communications networks and services shall be permitted to process electronic communications data only if:

(...)

(b) it is necessary to maintain or restore the security of electronic communications networks and services, or detect technical faults and/or errors and/or security risks and/or attacks in the transmission of electronic communications, ~~for the duration necessary for that purpose;~~

(c) it is necessary to detect or prevent security risks and/or attacks on end users' terminal equipment, ~~for the duration necessary for that purpose.~~²⁵²

With regard to the basis for employees, the Council proposes in its latest version of 6 March 2020, in the renumbered recital 16c to strike its previous insistence of consent from employees as a legal ground.

Providers of electronic communications services may, for example, obtain the consent of the end-user for the processing of electronic communications data, at the time of the conclusion of the contract, and any moment in time thereafter. In some cases, the legal person having subscribed to the electronic communications service may allow a natural person, such as an employee, to make use of the service in accordance with Regulation 2016/679.

With regards to the use of the processing and storage capabilities of terminal equipment, the Council deleted explanations when consent would be required from recital 21:²⁵³

Use of the processing and storage capabilities of terminal equipment or to access to information stored in terminal equipment without the consent of the end-user should be limited to situations that involve no, or only very limited, intrusion of privacy. For instance, consent should not be requested for authorizing the technical storage or access which is strictly necessary and proportionate for the legitimate purpose of enabling the use of providing a specific service explicitly requested by the end-user. This may include the storing of cookies for the duration of a single established session on a website to keep track of the end-user's input when filling in online forms over several pages, authentication session cookies used to verify the identity of end users engaged in online transactions or cookies used to remember items selected by the end-user and placed in shopping basket. In the area of IoT services which rely on/deploy connected devices (such as connected thermostats, connected medical devices, smart meters or automated and connected vehicles), the use of the processing and storage capacities of those devices and access to information stored therein should not require consent to the extent that such use or access is necessary for the provision of the service requested by the end-user. For example, storing of information in or accessing information from a smart meter might be considered as necessary for the provision of a requested energy supply service to the extent the information stored and accessed is necessary for the stability and security of the energy network or for the billing of the end users' energy consumption (...)

~~*To the extent that use is made of processing and storage capabilities of terminal equipment and information from end users' terminal equipment is collected for other*~~

²⁵² Idem. This article was initially article 6 (1). The limitation of the duration of processing is included in a separate second section: "*Electronic [sic] communications data shall only be permitted to be processed for the duration necessary for the specified purpose or purposes according to Articles 6 to 6c and if the specified purpose or purposes cannot be fulfilled by processing information that is made anonymous.*"

²⁵³ Idem.

~~purposes than for what is necessary for the purpose of carrying out the transmission of an electronic communication over an electronic communications network or for the provision of the service requested, consent should be required. In such a scenario, consent should normally be given by the end user who requests the service from the provider of the service.~~

In sum, it appears that the consent requirement for the collection of information from devices that is not necessary to provide a service will continue to apply under the ePrivacy Regulation. In its most recent version the Council proposes to introduce the legitimate interest ground. This is diametrically opposed to the position of European Parliament and Commission. It therefore seems likely that the current ePrivacy Directive, which does not contain such a possibility to balance interests, will continue to apply in the next few years.²⁵⁴

10. Retention periods

Google provides limited public information about the retention periods for the different kinds of personal data it collects and stores.

10.1 Customer Data

Because of its nature (e.g. content of files, communications), there are no fixed retention periods applicable to Customer Data during the term of the G Suite Enterprise agreement. During the term of the G Suite Enterprise agreement, customers may request deletion of Customer Data. Google must comply with such request for a *hard delete* as soon as reasonably possible and in any event within a maximum period of 180 days. Upon termination of the G Suite Enterprise agreement, the customer may request the return of Customer Data or its deletion. Google will equally comply with such a request for a *soft delete* as soon as reasonably possible and in any event within a maximum period of 180 days.

10.2 Diagnostic Data

10.2.1 Audit logs

Google provides a good overview of the retention periods it applies to the different audit logs that administrators can access, as copied in the table below. Google explains that the retention time for any report or audit log not mentioned in the table, is 6 months.²⁵⁵

However, admins can decide to retain audit logs longer than the default retention periods: the retention period for exported Customer/User usage data through the Reports API is 15 months.

²⁵⁴ It is not clear when and if the new ePrivacy Regulation (2017/0003/COD) will enter into force. Progress can be tracked via: https://eur-lex.europa.eu/procedure/EN/2017_3 The Ministers of the Member States have not yet reached agreement in the Council (in July 2020) on their negotiating position on the ePrivacy Regulation. Thereafter, the trilogue should start negotiations with the (new) European Commission and the (new) European Parliament. Subsequently, a transitional period of 1 or 2 years will apply. In any case, the scope of the scope of the Telecommunications Directives and the ePrivacy rules will be extended via the Electronic Communications Code (2016/0288(COD), final vote by the European Parliament on 14 November 2018) after a transitional period of 2 years, at the end of 2020, from the current handful of providers of telephony and Internet services to all web-based equivalent providers.

²⁵⁵ Google, G Suite Admin help, Data retention and lag times, URL: <https://support.google.com/a/answer/7061566?hl=en>

Google audit log or report name	Default retention period
Admin audit log	6 months
Calendar audit log	6 months
Jamboard audit log	6 months
Google+ audit log	6 months
OAuth Token audit log (availability of these logs is dependent on your subscription, such as G Suite Enterprise)	6 months
Devices audit log (availability of these logs is dependent on your subscription, such as G Suite Enterprise)	6 months
SAML audit log	6 months
Drive audit log (availability of these logs is dependent on your subscription, such as G Suite Enterprise)	6 months
Email log search	30 days
Account activity reports	6 months
Security reports	6 months
Groups audit log	6 months
Chat audit log	6 months
Meet audit log	6 months
Voice audit log	6 months
User accounts audit log	6 months
Access Transparency	6 months
Audit data retrieved using the API	6 months
Customer/User usage data retrieved using the API	15 months
Entities usage data retrieved using the API	30 days

10.2.2

Other Diagnostic Data (telemetry, website data, use of Google Account and Additional Services)

As explained in the sections before, Google processes Diagnostic Data and data relating to Additional Services, the Google Account (unless used in conjunction with a Core Service) and Other related services such as Feedback under its (consumer) Privacy Policy.

Google does not publish a similar table with retention periods for Diagnostic Data other than the audit logs, but instead, refers to its (consumer) Privacy Policy. Google explains that in some cases, personal data are not deleted but anonymised by deleting parts of the data.

"We also take steps to anonymize certain data within set time periods. For example, we anonymize advertising data in server logs by removing part of the IP address after 9 months and cookie information after 18 months."²⁵⁶

If Google only removes a single octet from the IPv4 addresses, the resulting group of 255 possible end users may not prove to be anonymous, if for example law enforcement has urgent reasons to detect the identity of a specific person.

In response to questions raised during this DPIA, Google wrote:

"There is no single retention period for Diagnostic Data. The retention period for Diagnostic Data varies per use case. Whilst in general we do not retain Diagnostic Data for longer than 180 days, some Diagnostic Data is retained for shorter periods

²⁵⁶ Google general Privacy Policy, Retaining your information, and: How Google retains data we collect, URL: <https://policies.google.com/technologies/retention?hl=en-US>

and other Diagnostic Data is retained for much longer periods (e.g. account deletion events).²⁵⁷

Google also confirmed that G Suite admins are *"not able to customize retention periods for Diagnostic Data (including telemetry and SIEM data)."*

Google explained:

"Our technical infrastructure that performs log anonymization and deletion is not designed to have direct access to information identifying the customer. All retention is governed by the retention rule provided by Google engineering when configuring each multi-tenant log."

It follows from Google's response to part A of the DPIA that Google stores Diagnostic Data in a central log repository. Google also explained it distinguishes between temporary and archival logs.

- *"Temporary Logs: short term logs which are retained only for a fixed period of time and then deleted*
- *Personal Logs: longer term logs which are keyed to internal end user Id and where end users have control over retention*
- *Archival Logs: long term anonymous logs and abuse system logs*

For Extended Retention Logs, our policy is to anonymize any data containing IP addresses within 9 months of when it was logged, and any other cookie-based data within 18 months unless these logs are maintained in connection with abuse systems (in which case, we may need to retain such data for longer periods)."²⁵⁸

All other information Google provided about its retention periods is marked by Google as confidential.

After completion of this report, on 12 November 2020 Google published the Google Cloud Privacy Notice. This notice does not contain any specific retention periods for the Customer Data or for the Diagnostic Data.²⁵⁹

²⁵⁷ From responses provided by representatives of Google to SLM Microsoft Rijk during the course of this DPIA.

²⁵⁸ Idem

²⁵⁹ Google, Google Cloud Privacy Notice, 7 December 2020, URL: <https://cloud.google.com/terms/cloud-privacy-notice>

Part B. Lawfulness of the data processing

The second part of this DPIA assesses the lawfulness of the data processing. This Part B contains an assessment of the legal grounds for processing (Section 11), the processing of special categories of personal data (Section 12), the principle of purpose limitation (Section 13) an assessment of the necessity and proportionality of the processing (Section 14), and data subject rights (Section 15).

11. Legal Grounds

To be permissible under the GDPR, processing of personal data must be based on one of the legal grounds mentioned in Article 6 (1) GDPR. Processing covers a wide range of operations performed on personal data, such as the collection, organisation, storage, alteration, retrieval, use, disclosure by transmission, making available, combination, restriction, erasure or destruction. Essentially, for processing to be lawful, the GDPR requires that the data controller bases the processing on the consent of the data subject, or on a legally defined necessity to process personal data. Data processors act on behalf of the data controller, and as such, can rely on the purposes and legal grounds that the data controller has for the processing.

The assessment of available legal grounds (sometimes called 'lawful bases') is tied closely to the principle of purpose limitation. The EDPB notes that "*The identification of the appropriate lawful basis is tied to principles of fairness and purpose limitation. [...] When controllers set out to identify the appropriate legal basis in line with the fairness principle, this will be difficult to achieve if they have not first clearly identified the purposes of processing, or if processing personal data goes beyond what is necessary for the specified purposes.*"²⁶⁰

Thus, in order to determine whether a legal ground is available for a specific processing operation, it is necessary to determine for what purpose, or what purposes, the data was or is collected and will be (further) processed. There must be a legal ground for each of these purposes.

The appropriate legal ground may depend on Google's role as joint data controller, or as data processor. Although it may be possible that the processing for specific purposes identified in this DPIA can be based on a legal ground, the lack of purpose limitation makes it impossible to determine whether the data are also processed for other purposes. For example, the transmission of Customer Data to Google for the specific purposes of technically providing a Core Service and keeping a Core Service and the data secure and up to date, might be based on a legal ground such as the performance of a contract between the government organisation and the employee. However, due to the lack of purpose limitation, the transmission of these data is currently based on a broad, non-specific purpose. Without a specific purpose or specific purposes, it is impossible to identify an appropriate legal ground.

As further described in the Sections 16 and 17, Google can fix these problems to a certain extent by contractually limiting the processing to clearly defined, specific purposes, and specifically excluding (further) processing for other purposes.

²⁶⁰ EDPB, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects - version adopted after public consultation, 16 October 2019, URL: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_en.

In the current circumstances the analysis of the legal grounds results in the conclusion that no legal grounds apply for any data processing.

This Section addresses four of the different possible legal grounds for the different purposes of the processing, in short: consent, contract with the data subject, public interest and legitimate interest. The legal ground of vital interest is not discussed, since neither Google nor Dutch government organisations have a vital (lifesaving) interest in processing personal data via G Suite Enterprise. Additionally, though Dutch government organisations may have to process digital information and communicate per e-mail, there is no legal obligation to use G Suite Enterprise.

Section 11.1 below describes the legal grounds government organisations may have for the processing of personal data in Customer Data from the Core Services, the Features and the Google Account when used in conjunction with the Core Services. This section distinguishes between Google's intended role as data processor, and Google's factual role as joint controller with the government organisations.

Section 11.2 describes the legal grounds for the processing of Customer Data from the Additional Services, the Technical Support Services, the Other Related Services and all Diagnostic Data. This section is based on the analysis that government organisations and Google currently act as joint controllers for these personal data. This means the government organisations must have a legal ground for each purpose for which Google processes these personal data.

Section 11.3 briefly describes the legal grounds for Google to process limited personal data about customers as an independent data controller. This can be the case if Google uses contact and license data to send invoices, or when Google has to comply with a legal request from a law enforcement authority and is prohibited (with a *gagging order*) from forwarding this request to its customer.

11.1 Customer Data from the Core Services, Features and the Google Account used in the Core Services

As detailed in Section 4.2 of this report, Google does not offer an exhaustive list of specific and explicit purposes for which Google as a data processor necessarily has to process personal data in the Customer Data in the Core Services. Google claims it only acts on the 'documented instructions' of its customers.

This DPIA shows that Google factually processes the personal data in the Customer Data in the Core Services for at least 8, and possibly 20 purposes. These purposes are not specifically and explicitly enumerated as part of the documented instructions of the data controller. Google seems to deem these other purposes compatible with the catch-all purpose. As will be analysed in more detail in Section 13 of this report, the processing of personal data in the context of the G Suite Enterprise services currently does not comply with the principle of purpose limitation.

Even if Google contractually guarantees its role as data processor for the personal data processed through the Features and Google Account when used in conjunction with a Core Service,²⁶¹ the same lack of purpose limitation applies.

Without a specific purpose or specific purposes, it is impossible for government organisations to identify any appropriate legal ground.

If Google would indeed be a data processor, Google would be able to rely on the purposes and legal grounds for processing of the government organization. However, as explained in the Sections 5.2 and 5.4, Google does not qualify as a data processor.

²⁶¹ See Sections 1.4.2 and 1.4.3 of this report.

Google and the government organisations are joint controllers, and this means the government organisations must have a legal ground for each purpose for which Google processes the personal data.

11.1.1

Consent

Article 6 (1) (a) GDPR reads: “the data subject has given **consent** to the processing of his or her personal data for one or more specific purposes”

Article 4(11) GDPR defines consent as “consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.”

As explained above, government organisations can currently not rely on any legal ground for the processing of personal data in the Customer Data in the Core Services, the Features and the Google Account when used in conjunction with the Core Services. This includes the legal ground of consent.

Even if Google and government organisations would agree on appropriate purpose limitation (as further discussed in Section 17), government organisations still cannot rely on consent as a legal ground, as explained below.

Government organisations should refrain from asking for consent from employees for the processing of their personal or confidential data. In view of the imbalance of power between employees and employers, consent can seldom be given freely.²⁶² Employees may not be free to refuse or withdraw consent for the processing of their personal data without facing adverse consequences.

The fact that government organisations are public authorities also makes it difficult to rely on consent for processing. In the context of Recital 43 of the GDPR, the EDPB explains: “*whenever the controller is a public authority, there is often a clear imbalance of power in the relationship between the controller and the data subject. It is also clear in most cases that the data subject will have no realistic alternatives to accepting the processing (terms) of this controller. The EDPB considers that there are other lawful bases that are, in principle, more appropriate to the activity of public authorities.*”²⁶³

Another reason why consent is not a possible legal ground in this case, is that the Customer Data may contain personal data from other employees or other data subjects who may have had to provide personal data to, and communicate with, the Dutch government following a statutory obligation.

Government organisations are not able to invite these other individuals to provide valid consent to Google for the processing of their personal data as part of the Customer Data.

There are more reasons why government employees are currently not in a position to provide valid consent for the processing of their personal data through G Suite Enterprise. These relate to the requirements of specific, well-informed consent and the requirements of the ePrivacy Directive with regard to cookies and similar tracking technologies.

²⁶² Recital 49 of the GDPR: “*In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case **where there is a clear imbalance between the data subject and the controller**, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation.*”

²⁶³ EDPB, *Guidelines on consent*, paragraph 3.1.1.

Google and government organisations as joint controllers

Because Google does not act as a data processor for these data, it must rely on its own legal ground. In its current role as joint controller with the government organisations, Google does not obtain valid consent for the processing either.

As explained in Section 1.4.2, Google requires the creation of a Google Account as a prerequisite to the use of the G Suite Enterprise services. The end user must click an 'Accept' button, referring to the Terms of Service and the (consumer) Privacy Policy. This does not meet the requirements of consent of the GDPR, for multiple reasons.

First, there is no specific and informed indication of the data subject's wishes. As explained in Sections 4.2 and 4.3, the (consumer) Privacy Policy lists non-limitative, list of purposes that are not specific nor explicit. End users do not know what they are agreeing to.

Second, merely clicking the 'Accept' button is not an indication that consent is freely given. There is no 'Do not accept' button. End users cannot use the G Suite Enterprise services if they do not accept the Terms of Service. Yet, their employer requires them to use the services in the context of their employment.²⁶⁴ Furthermore, the conflation of several purposes in the (consumer) Privacy Policy, without any attempt to seek granular consent, leads to a lack of freedom of choice for the data subject.²⁶⁵

Third, the indication is ambiguous, not given by a clear affirmation and not specific. The EDPB explains: 'A controller must also beware that consent cannot be obtained through the same motion as agreeing to a contract or accepting general terms and conditions of a service. Blanket acceptance of general terms and conditions cannot be seen as a clear affirmative action to consent to the use of personal data'.²⁶⁶ As explained above, the 'Accept' button in Google's welcome notice is a catch-all agreement to many terms.

Google's procedure with regard to obtaining consent was the subject of a recent ruling of France's highest administrative court, the Council of State. The court rejected Google's appeal against a 50 million dollar fine imposed by the CNIL, the French Data Protection Authority.²⁶⁷ The fine was imposed because of a lack of consent for the use of personal data for advertising purposes when creating a Google Account on an Android device.

In paragraphs 22 and 23 the court summarises the problems with consent (emphasis added by the author):

22. (...) in order to create a Google Account necessary for the use of the Android operating system, the user is first presented with the 'Privacy Policy and Terms of Use', which briefly and very generally inform him or her of the nature of the data processed and the purposes of the processing carried out by Google. The user can then click on a "more options" link or tick the boxes "I accept the Google terms of use" and "I agree that my information will be used as described above and detailed in the Privacy Policy" to create his or her account. If the user clicks on the "more

²⁶⁴ This could be different if government organisations would offer their employees an alternative to the use of G Suite Enterprise. However, it is extremely unlikely that this will occur due to financial, security, operational and legal reasons.

²⁶⁵ EDPB, *Guidelines on consent*, paragraph 3.1.3.

²⁶⁶ EDPB, *Guidelines on consent*, paragraph 3.4.

²⁶⁷ Press release Council of State 19 June 2020, (in French) RGPD : le Conseil d'État rejette le recours dirigé contre la sanction de 50 millions d'euros infligée à Google par la CNIL, URL: <https://www.conseil-etat.fr/actualites/actualites/rgpd-le-conseil-d-etat-rejette-le-recours-dirige-contre-la-sanction-de-50-millions-d-euros-infligee-a-google-par-la-cnil>. Decision: <https://www.conseil-etat.fr/ressources/decisions-contentieuses/dernieres-decisions-importantes/conseil-d-etat-19-juin-2020-sanction-infligee-a-google-par-la-cnil>

options" link, a page will prompt the user to set up their account. Under the title 'personalization of ads', a pre-ticked box, which he can uncheck, indicates that he agrees to display personalized ads. More information can be obtained by clicking on a "learn more" link, which specifies how to display personalized ads, but this information is not exhaustive. However, if the user does not choose to click on the "more options" link on the first page presented to them, a "simple confirmation" window will appear, reminding the user that the account is configured to include personalization features "such as recommendations and personalized ads". This page tells the user how to change these settings. The user can then return to the "more options" page or definitively confirm the creation of their account.

23. While the architecture described in the previous point means that the user is always invited to indicate that he agrees to his information being processed in accordance with the default settings of his account, i.e. including functions for personalizing the advertisements, the information available to him for this purpose is general and diluted in the middle of purposes that do not necessarily require consent as a legal basis, both at the first level of information and in the window entitled "simple confirmation". It thus appears that the information on the scope of the data processing for "targeted advertising" purposes provided at the first level is, in the light of the clarity and accessibility requirements recalled above, insufficient. In the absence of sufficient prior information, the consent collected in a global manner for all purposes, including this one, cannot be regarded as informed nor, consequently and in any case, as valid. If additional information on the targeted advertising purpose is provided at the second level (by clicking on "More options") and a specific consent for this purpose is then collected, it appears that this information is itself insufficient in view of the scope of the processing. Finally, consent is collected by means of a pre-checked box. In these circumstances, the CNIL's restricted panel rightly considered that the methods of collecting consent do not meet the requirements of the GDPR, which require a clear positive act, without the alleged circumstance that the regulation does not require separate collection of consent for the purpose of advertising targeting having any bearing on this point. (...)

Even though the sign-up procedure for a Google Account in the G Suite Enterprise environment is slightly different, as it involves a one-off pop-up Welcome notice with reference to the Terms of Service and (consumer) Privacy Policy (Figure 6 in this report), Google equally fails to collect valid consent from end users. Google similarly asks for consent in a global manner for all purposes and all kinds of personal data and does not provide sufficiently precise and centrally organised information.

As explained above, even if Google would ask for consent in a specific, unambiguous manner, Google can never comply with the requirement that the affirmation is freely given, because end users have no choice but to accept the (consumer) Privacy Policy. Therefore, Google cannot rely on consent of the data subject with respect to the personal data in Customer Data relating to the Google Account of end users.

11.1.2

Contract

Article 6 (1) (b) GDPR reads: "processing is **necessary for the performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract."

The legal ground of necessity for the performance of a contract is limited to situations where organisations have an employment contract with specific data subjects, and the processing is strictly necessary to perform the contract with such individual data subjects. The European Data Protection Authorities explain: "The controller should be able to demonstrate how the main object of the specific contract with the data

*subject cannot, as a matter of fact, be performed if the specific processing of the personal data in question does not occur. Thus, this ground can never be invoked by a party that does not have its own contract with that individual.”*²⁶⁸

As explained above, government organisations can currently not rely on any legal ground for the processing of personal data. This includes the legal ground of necessity to perform a contract.

Government organisations may provide employees with the G Suite Enterprise services to carry out the tasks included in their job description. As described in Section 6.1 of this report, Dutch government organisations have an interest in the ability for employees to seamlessly work at home with online collaboration tools, even more urgent since the outbreak of the COVID-19 pandemic.

To be able to successfully invoke this legal ground with respect to government end users (employees, civil servants), the processing of the personal data in the Customer Data from the Core Services, the Features and the Google Account has to be strictly necessary for the performance of the contract with each individual data subject.

In practice, if a government organisation allows its employees (or other temporary workers) to use Gmail, it is inevitable that the government organisation also processes personal data about other data subjects who do not have a contractual relation with that government organisation.

The second, equally important, reason why this legal ground is not available, is because the processing has to be necessary in relation to each individual employee. The EDPB explains: *“the controller should be able to demonstrate how the main subject-matter of the specific contract with the data subject cannot, as a matter of fact, be performed if the specific processing of the personal data in question does not occur. The important issue here is the nexus between the personal data and processing operations concerned, and the performance or non-performance of the service provided under the contract.”*²⁶⁹

Taking this into account, government organisations may only base the processing on the legal ground of necessity to perform a contract with all of its employees if the processing is required in order to comply with the agreement. What purposes are necessary must be assessed on a case-by-case basis. Examples of purposes that may be necessary are:

- Technically delivering the Core Services, the Features and the Technical Support Services;

²⁶⁸ EDPB Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, paragraph 30. See also paragraph 26: *“A controller can rely on Article 6(1)(b) to process personal data when it can, in line with its accountability obligations under Article 5(2), establish both that the processing takes place in the context of a valid contract with the data subject and that processing is necessary in order that the particular contract with the data subject can be performed [emphasis added by Privacy Company].”* And paragraph 28: *“the EDPB endorses the guidance previously adopted by WP29 on the equivalent provision under the previous Directive that ‘necessary for the performance of a contract with the data subject’: ... must be interpreted strictly and does not cover situations where the processing is not genuinely necessary for the performance of a contract, but rather unilaterally imposed on the data subject by the controller. Also the fact that some processing is covered by a contract does not automatically mean that the processing is necessary for its performance. [...] Even if these processing activities are specifically mentioned in the small print of the contract, this fact alone does not make them ‘necessary’ for the performance of the contract.”*

²⁶⁹ EDPB, Guidelines on processing under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, paragraph 2.4.

- with respect to end users: enabling the use of the Core Services through the Google Account;
- processing Customer Data from end users or administrators to provide Technical Support Services upon their request (but not for the Customer Data relating to other data subjects);
- with respect to admins and end users: following their instructions expressed by privacy settings .

Other purposes, for example relating to security, may not require the processing of data of all individual employees. In that case, government organisations should rather rely on the ground of necessity for the public or legitimate interest for this purpose.

Because G Suite Enterprise involves processing personal data of individuals that do not have a contract with the Dutch government, and Google does not allow its government customers to limit the data processing to the three valid contractual purposes, government organisations cannot successfully claim the legal ground of necessity for the performance of the contract for the processing of the Customer Data through G Suite Enterprise.

In sum, the legal ground of contract cannot be invoked by government organisations for the processing of personal data of data subjects that do not have a contractual relationship with that government organisation. Furthermore, government organisations cannot invoke the legal ground of contract for the processing of personal data for purposes that are not necessary for the performance of the contract with each individual data subject.

Google and government organisations as joint controllers

Because Google does not act as a data processor for these data, it must rely on its own legal ground. In its current role as joint controller with the government organisations, Google cannot rely on the legal ground performance of a contract.

In the Welcome notice for new end users, Google writes: *'If your organisation provides you access to the G Suite core services, your use of those services is governed by your organisation's G Suite agreement*'.

According to Google, the use of the Core Services is covered by the G Suite Agreement. As this is not a contract between Google and the end user, Google cannot invoke 'performance of a contract' as the legal ground for the processing of personal data from the Core Services.

Google further writes: *'Any other Google services your administrator enables ("Additional Services") are available to you under the Google Terms of Service and the Google Privacy Policy. Certain Additional Services may also have service-specific terms. Your use of any services your administrator allows you to access constitutes acceptance of applicable service-specific terms*'.

The Features are not included in the list of service-specific terms. Thus, although they were not (yet) covered by the G Suite DPA at the time of completion of this DPIA, they were also not covered under the Terms of Service. As the Features are not provided under a contract between Google and the end user, Google cannot invoke 'performance of a contract' as the legal ground for the processing of personal data from the Features either.

As cited in Section 1.4.3 of this report, Google claims it has a direct contractual relationship with end users for the purposes of the Google Account. By accepting these terms, end users enter into a direct agreement with Google, according to

Google.²⁷⁰ This is incorrect. Under Dutch law, which applies to the offering of the Terms of Service to Dutch individuals²⁷¹, the conclusion of an agreement requires the acceptance of an offer. Such acceptance is only valid if it is based on that party's will. As described above, end users have no choice but to click the 'Accept' button. If they do not accept, they cannot use the G Suite Enterprise services. Yet, their employer requires them to use the services in the context of their employment. Google is aware of this, as it sends the individual an enterprise-related Welcome notice.

The situation can be compared to employees that have to participate in a work excursion to a physical bakery. Only after they have entered the shop, the baker tells them that by entering his space, they have agreed to a contract to each buy 10 loaves of bread.

As a result of the lack of choice and the inability of end users to freely accept the Terms of Service, no agreement comes into force. As the Google Account is not governed by a contract between Google and the end user, Google cannot invoke 'performance of a contract' as the legal ground for the processing of personal data from the Google Account.

Google can also not use the legal ground performance of a contract in other situations where it does not have a contract with the relevant data subject, such as data subjects that communicate with a government organisation. This does not change if a data subject has a consumer contract with Google, as the processing by Google in the context of the G Suite Enterprise services is not necessary for the performance of that specific consumer contract.

11.1.3

Public interest

Article 6 (1) (e) GDPR reads: "*processing is necessary for the **performance of a task carried out in the public interest** or in the exercise of official authority vested in the controller.*"

As explained above, government organisations can currently not rely on any legal ground for the processing of personal data. This includes the legal ground of necessity for the public interest.

The use of digital productivity and communications tools can be necessary to perform tasks carried out by government organisations in the public interest. This is certainly the case if an organisation needs to answer a digital request from a citizen relating to the performance of their public interest tasks.

As the EDPB notes in a letter to the European Commission on the use of contract tracing apps relating to the COVID-19 pandemic, even if data subjects voluntarily submit personal data, the processing by a government organisation can still be based on this legal ground. It does not have to be based on consent.

"The EDPB notes that the mere fact that the use of the contact tracing takes place on a voluntary basis, does not mean that the processing of personal data by public authorities necessarily be based on the consent. When public authorities provide a service, based on a mandate assigned by and in line with requirements laid down in

²⁷⁰ Google reply to part A of the DPIA.

²⁷¹ Article 6 Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I).

law, it appears that the most relevant legal basis for the processing is the necessity for the performance of a task for public interest.”²⁷²

The legal ground of public interest should be used in combination with the necessity to perform the (employment)contract and, as will be assessed below, in limited cases, also for the necessity for the legitimate interest of the government organisations.

Google and government organisations as joint controllers

Because Google does not act as a data processor for these data, it must rely on its own legal ground. In its current role as joint controller with the government organisations, Google cannot rely on the legal ground of ‘public interest’, as Google does not carry out any public tasks.

11.1.4

Legitimate interest

Article 6 (1) (f) GDPR reads: *“processing is **necessary for the purposes of the legitimate interests pursued by the controller** or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.”*

The last sentence of Article 6(1) of the GDPR adds: *“Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.”*

As explained above, government organisations can currently not rely on any legal ground for the processing of personal data. This includes the legal ground of necessity for their legitimate interest.

The general prohibition for government organisations (as data controllers) to process personal data based on the necessity for their legitimate interest does not completely render this legal ground useless for them. Government organisations may also process personal data in a different role, outside of the tasks they carry out in the public interest, for example, when they hire office space or pay salaries to employees.

Recital 47 of the GDPR explains: *“Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or **in the service of the controller.**”*

In order to keep the personal data in Customer Data secure, it may be necessary for government organisations to (instruct Google to) create aggregated data and statistics, across all of its Enterprise customers, and to detect and solve new information security risks. It can equally be necessary for government organisations to (instruct Google to) to analyse personal data in Customer Data in the context of Technical Support Services, at the request of an admin.

If a government organisation can successfully invoke the legal ground of legitimate interest for the Dutch government organisations, must be assessed on a case-by-case basis. The proportionality of the processing plays a crucial role. This will be elaborated in Section 14.2 of this report. In any event, government organisations must ensure *“that the interests or the fundamental rights and freedoms of the data*

²⁷² https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf

subjects are not overriding, taking into account the reasonable expectations of data subjects based on their relationship with the controller” (Recital 47 GDPR).

In sum, as Google does not enable government organisations to comply with their obligations under the principle of purpose limitation, government organisations currently do not have any legal ground for the processing of personal data in Customer Data from the Core Services, the Features and the Google Account.

11.2 Personal data in Additional Services, Other related services, Technical Support Services and all Diagnostic Data

As explained above, the processing of personal data in the context of G Suite Enterprise currently does not comply with the principle of purpose limitation. The G Suite DPA does not cover the processing of personal data in the Additional Services, the Google Account (when not used in conjunction with a Google Account), the Technical Support Services²⁷³ and the Other related services. The contractual guarantees equally do not apply to any Diagnostic Data.

Google does not make clear and comprehensive information available with respect to the processing of these personal data in an enterprise context. Google states that its (consumer) Privacy Policy applies to the majority of these data. In its Privacy Policy Google qualifies itself as a data controller. However, as analysed in Section 5.4, Google and the government organisations are joint controllers.

As explained in Sections 4.2 and 4.3 of this report, the (consumer) Privacy Policy contains a non-limitative list of 33 purposes that are not specific nor explicit, plus additional specific purposes for the Chrome OS and Chrome browser. Without a specific purpose or specific purposes, it is impossible for government organisations to identify any appropriate legal ground. After completion of this report, On 12 November 2020 Google published a Google Cloud Privacy Notice with a list of purposes for the Diagnostic Data.²⁷⁴

11.2.1 Consent

As explained above, government organisations can currently not rely on any legal ground for the processing of personal data. This includes the legal ground of consent.

Section 11.1.1 above explains why Google cannot rely on the legal ground of consent for the processing of personal data through the Core Services, the Features and the Google Account. The same analysis also applies to the processing of personal data in the Additional Services, the Technical Support Services, the Other related services and all Diagnostic Data.

As described in Section 3.2 of this report, the Additional Services are all switched On by default for G Suite Enterprise customers. It thus requires an active intervention from admins or end users to block access to these services. As analysed in Section 5.3.3, with the use of these default settings Google benefits from cognitive limitations that prevent admins and end users from making any changes to the default settings, even if those settings do not match their privacy interests. The failure to actively object against these settings cannot be construed as ‘consent.’

²⁷³ Google calls this ‘Support Data’ in the Technical Support Services Guidelines. According to the G Suite DPA, Google processes the Customer Data in the Technical Support Services as data processor. However, the G Suite DPA does not apply to Customer Data when they are provided as Support Data to Google in the context of the Technical Support Services. See Sections 1.4.4 and 5.3.5.

²⁷⁴ Google, Google Cloud Privacy Notice, 7 December 2020, URL: <https://cloud.google.com/terms/cloud-privacy-notice>

Google's failure to obtain valid consent for the Diagnostic Data is especially problematic in relation to the collection of information from end user devices through telemetry data and cookies. As explained in Section 9 of this report, article 11.7a of the Dutch Telecommunications Act (based on the ePrivacy Directive) in principle obliges website owners to obtain valid informed consent prior to retrieving or placing information on an end user device, such as cookies in a browser. However, consent is not required if the cookies (or similar information) are necessary for the technical operation of a site or online service, or if the cookies do not infringe on users' privacy rights, or only to a very limited extent.

The applicability of the GDPR does not exclude applicability of the Dutch Telecommunications Act with regard to cookies and similar technologies. As described in Section 2.3, Google collects personal data from Android devices, the Chrome OS and the Chrome browser in the form of unique end user and device information, combined with potentially sensitive Customer Data (for example a sentence in the *Enhanced Spellcheck*) and behavioural information such as app usage and the use of biometric authentication with timestamps. Google does not inform data subjects about the collection of these data, and does not obtain separate consent. Because these telemetry data are not strictly necessary to operate its services, and does infringe on the fundamental rights of data subjects, Google fails to obtain the legally required consent

As joint controllers, Google and the government organisations cannot rely on consent, even though such consent is required by the Dutch Telecommunications Act when these personal data are processed for commercial communication, personalised marketing and tracking purposes. Google does not ask for consent for the retrieval of unique identifiers from the Chrome OS and the Chrome browser, nor for the reading of telemetry data (Diagnostic Data).

11.2.2 *Contract*

As explained above, government organisations can currently not rely on any legal ground for the processing of personal data. This includes the legal ground of performance of a contract.

As explained in Section 11.1.2, government organisations can base processing on the legal ground 'performance of a contract' when they have a (labour) contract with the relevant data subject and the processing is necessary to perform their obligations in relation to each data subject. Processing for the purpose of technically providing the Core Services can likely be based on this legal ground. This can also be the case for the Technical Support Services and services that provide essential functionality, such as Features. This includes the processing of both Customer Data and Diagnostic Data, but only if the processing is necessary for the execution of the contract with each individual data subject.

Reliance on the legal ground of 'performance of a contract' requires adequate purpose limitation to ensure that the personal data will not be processed for other purposes for which no legal grounds are available. Without purpose limitation, it remains impossible to ascertain what the purposes of processing are, and thus whether a legal ground can apply with respect to all purposes.

11.2.3 *Public interest*

As explained above, government organisations can currently not rely on any legal ground for the processing of personal data. This includes the legal ground of 'public interest'.

As a side note, as described in Section 3.1.5, Google has used the location history of end users that have turned on the Additional Service 'Location History' to

proactively publish statistics “to help public health officials combat COVID-19.” Google cannot process personal data on the legal ground of public interest, because Google does not carry out any public tasks. Google did not process these location data as processor at the request of government organisations either. Since G Suite Enterprise end users were not made aware of such further processing of their location data prior to enabling this setting, Google cannot base this processing on consent either.

11.2.4 *Legitimate interest*

As explained above, government organisations can currently not rely on any legal ground for the processing of personal data. This includes the legal ground ‘legitimate interest’.

As joint controllers with Google, Dutch government organisations may (instruct Google to) process a limited set of innocent Diagnostic Data on the basis of the necessity for their legitimate interest, if the data processing is not necessary to perform a public task. This can be the case for the following purposes:

- detect and solve new information security risks
- process the data according to the settings chosen by the administrators
- use Diagnostic Data to provide Technical Support, when an admin asks for this help
- keep the service functioning and up-to-date (providing automatic product updates; and
- determine the account status and ads personalisation preferences [cookies].

Government organisations may also rely on this legal ground for the (limited) use of some Diagnostic Data for (security) analytics, as long as the rights and freedoms of the end users and other data subjects do not prevail over this interest. However, government organisations may not allow further processing of the Diagnostic Data obtained from devices and browsers for any purpose that involves tracking and profiling of end users and end user behaviour. Such a purpose would require consent based on the ePrivacy Directive, and employees are not free to give such consent.

As mentioned above for the ground of ‘public interest’, reliance on the legal ground of ‘legitimate interest’ requires adequate purpose limitation. Without a specific purpose or specific purposes, it is impossible to identify an appropriate any legal ground, including ‘legitimate interest’.

In sum, as joint controllers for the processing of the personal data in the Additional Services, the Technical Support Services, the Other related services and all Diagnostic Data, nor Google nor the government organisations have a legal basis for the processing under the current circumstances.

11.3 **Google’s own legitimate business purposes**

In some cases, Google processes personal data as an independent data controller, for example for the processing of the number of accounts and sold licenses for annual financial statements, and the sending of invoices. These purposes for the processing need to be clearly defined in the contract with the Dutch government organisations.

Google may be ordered to hand over personal data to a law enforcement authority, security agency or secret service. It follows from the G Suite DPA that Google will refer disclosure requests with regard to personal data in Customer Data from the Core Services to the government organisation, unless “the law prohibits Google from doing so on important grounds of public interest”. In those circumstances, Google

can act as a data processor. When Google refers disclose requests to its customer, Google acts as a data processor. However, if Google is ordered to disclose data itself, and is prohibited with a *gagging order* from informing the customer, Google acts as a data controller when it hands over personal data (be it Customer Data or Diagnostic Data).

As explained in Section 5.3.7, government organisations cannot instruct Google as a data processor to comply with legal obligations for which they do not have a legal ground, as this would violate the GDPR. Google's compliance with a government order from a country with which the Netherlands or the EU do not have a Mutual Legal Assistance Treaty, such as is the case for the USA, would be in violation of the GDPR. Therefore, Google must take its responsibility and take its role as independent data controller for disclosure in these particular circumstances.

12. Special categories of data

Special categories of data are "*personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation*" (Article 9 GDPR). In addition, Article 10 of the GDPR prohibits the processing of "*personal data relating to criminal convictions and offences or related security measures.*"

As explained in Section 2.5.1 of this DPIA, it is up to the individual government organisations to determine if they process special categories of personal data. Government organisations must determine if the specific data protection risks associated with the storing of these data on Google's cloud computers (for example, storing of documents in Drive, recordings in Google Meet, processing through Gmail) require additional protection measures.

The data protection risks for data subjects are not limited to the processing of special categories of personal data. Similar risks may apply to other categories of personal data of a sensitive nature, classified or secret data. The EDPS explains in its guidelines on the use of cloud computing services by European institutions that special categories of personal data should be interpreted broadly when interpreting the risks for data subjects. The EDPS writes: "*Nevertheless, this is not the only factor determining the level of risk. Personal data that do not fall under the mentioned categories might lead to high levels of risk for the rights and freedoms of natural persons under certain circumstances, in particular when the processing operation includes the scoring or evaluation of individuals with an impact on their life such as in a work or financial context, automated decision making with legal effect, or systematic monitoring, e.g. through CCTV.*"²⁷⁵ The EDPS also refers to the criteria provided by the Article 29 Working Party when a Data Protection Impact Assessment (DPIA) is required.²⁷⁶

Government organisations must consider the risk that special categories of personal data (or otherwise sensitive data) could end up in file and path names in the Drive

²⁷⁵ EDPS, Guidelines on the use of cloud computing services by the European institutions and bodies, 10 March 2018, URL: https://edps.europa.eu/sites/edp/files/publication/18-03-16_cloud_computing_guidelines_en.pdf

²⁷⁶ Article 29 Working Party (now: EDPB), WP 248 rev.01, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, URL: http://ec.europa.eu/newsroom/Article29/item-detail.cfm?item_id=611236 .

Audit log file, in combination with the email address of the employee. Google processes these data in its role as processor, as well as in its role as joint data controller.

The technical research in this DPIA shows that Google also collects Customer Data in sentences and words from the *Enhanced Spellingchecker* in telemetry data from the Chrome browser.

Government organisations should therefore take account of the general prohibition on the processing of special categories of personal data from articles 9 and 10 of the GDPR if they are joint controllers with Google. There is no exception for the processing of these personal data by Google for its own 33 purposes. The only general useful exception in Article 9 GDPR is if the data subject has given explicit consent. However, valid consent is not an option as explained in sections 11.1.1 and 11.2.1 of this DPIA. Article 10 of the GDPR completely prohibits the processing of personal data relating to criminal convictions and offences, if not under the control of official authority or when authorized by Union or member law.

12.1 Transfer of special, sensitive, secret and confidential data to the USA

In G Suite Enterprise admins can elect to store Customer Data from certain Core Services only in data centres in the European Union. This choice is not available for the Customer Data from other Core Services, the Google Account, the Additional Services, Support Data and any Diagnostic Data. Those data may therefore be stored anywhere where Google maintains facilities. With regard to the transfer of personal data in Customer Data to the USA, customers can accept the SCC, as described in Section 7. At the time of completion of this DPIA report, all other transfers of personal data outside of the EEA generally relied on the EU-US Privacy Shield.

The transfer and storage of personal data in the USA carries a risk of unlawful further processing of personal data (i) through interception or silent orders from USA law enforcement authorities, security agencies and secret services, (ii) through rogue administrators at Google and at subprocessors (only for the Technical Support Services), and (iii) by hostile state actors. The likelihood and impact of these risks are assessed in Section 16.2.12 of this report.

To mitigate some of these risks, government organisations can create policy rules to prevent that very confidential or state secret data are processed through cloud services. They could also draft a policy to prohibit the use of directly identifying personal or confidential data in file and path names. Google does not offer separate encryption possibilities for data stored in Drive, but customers may apply their own encryption from other companies before uploading sensitive data to Drive.²⁷⁷

In a whitepaper about encryption, Google explains that data on disks and backup media belonging to customers are always encrypted. Google has a distinct approach to encryption for each system, to mitigate the specific security risks.

Google automatically encrypts Customer Data stored on disks in the G Suite product family as it is written to disk with a per-chunk encryption key that is associated with a specific Access Control List. This means that different chunks are encrypted with different encryption keys, even if they belong to the same customer.²⁷⁸

²⁷⁷ In the G Suite Marketplace, different third-party encryption tools are available, URL: <https://gsuite.google.com/marketplace/search/encrypt>

²⁷⁸ How Google Uses Encryption to Protect Your Data, G Suite Encryption Whitepaper, URL: <https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf>

Technically, this works as follows: *“Each chunk key is encrypted by another key known as the wrapping key, which is managed by a Google-wide key management service (KMS). The result is a “wrapped” (encrypted) chunk key, which is stored alongside the encrypted data. The wrapping keys, needed to decrypt wrapped chunk keys, and therefore to decrypt the chunk, are known only to the KMS and are never stored at rest in unencrypted form. Data cannot be decrypted without both the wrapping key and the wrapped chunk key. Google has built a system to manage key rotation. (...) Chunk encryption keys and wrapping keys are rotated or replaced regularly.”*²⁷⁹

Additionally, Google describes it has rigorous procedures for assigning and removing access to the keys, and logging employee access to the keys and data.

These measures lower the risks of interception or unauthorised access to Customer Data, but do not eliminate them. These measures are not applied to Diagnostic Data.

13. Purpose limitation

The principle of purpose limitation is that data may only be *“collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes”* (Article 5 (1) (b) GDPR). Essentially, this means that the data controller must have a specified purpose for which personal data is collected, and can only process these data for purposes compatible with that original purpose.

Data controllers must be able to prove based on Article 5(2) of the GDPR that they comply with this principle (accountability). As explained in section 5.3 of this report, only data controllers may take decisions about the purposes, including purposes for further processing of the personal data. As a result, a data processor may not determine the purposes of the processing, nor what further processing it deems compatible with those original purposes.

Purpose limitation is the most difficult principle to comply with in big data processing, because it is precisely invented to gain new insights by combining data in a different way.

As described in the Sections 11.1 and 11.2 of this report, **currently nor Google nor the government organisations have a legal ground for any processing through G Suite Enterprise**. This is often caused by a lack of purpose limitation. In addition, the lack of an exhaustive list of specific and explicit purposes in the G Suite DPA leads to the qualification of government organisations and Google as joint controllers.

Note: After completion of this report, on 12 November 2020 Google published a Google Cloud Privacy Notice with a list of purposes.²⁸⁰The consequences of this publication are described in the new assessment of the risks added to the summary and conclusion of this report in January 2021.

As joint data controller for the Diagnostic Data, Google does not specify for what specific purposes it processes which personal data. As described in Section 4.3,

²⁷⁹ Idem.

²⁸⁰ Google, Google Cloud Privacy Notice, 7 December 2020, URL: <https://cloud.google.com/terms/cloud-privacy-notice>

Google mentions 33 purposes for data processing in its (consumer) Privacy Policy. Some purposes are so general (such as, for example, *Performing Research*, and *Combining information among all services and across devices to improve Google's services and the ads delivered by Google*) that the description offers no insight what processing Google does and does not permit itself to do under this purpose.

Based on the current contractual terms, Google may process Diagnostic Data collected about the use of the Core Services (including the Features), the Additional Services, the Technical Support Services and the Other related services, as well as the content from the Additional Services, use of the Google Account outside of the Core Services, for all 33 purposes mentioned in its (consumer) Privacy Policy. These purposes generally aim at serving Google's own commercial interests.

Google's long list of purposes in its role as data controller seems designed to maximise Google's liberty to process the personal data for new purposes and in new services. This allows Google to dynamically add (sub)purposes, or stop collecting Diagnostic Data for certain purposes. Without informing or asking consent from its end users, Google can change the telemetry and website data it collects. Google does not publish any documentation about the contents of the telemetry and website data it processes, other than an opaque description in its (consumer) Privacy Policy, and a list of telemetry events in a highly specialised source for Android developers. Google has not created any privacy controls to block or minimise the telemetry data, not for the data subjects, nor for admins. This lack of transparency makes it impossible for admins and end users to verify Google's privacy statements.

As data controller, Google does not publish any information about the parties with which it cooperates in the provision of its consumer services, except for a list of Google affiliates (group companies) included in the (consumer) Privacy Policy.²⁸¹ In its (consumer) Privacy Policy (which currently applies to the Google Account when not used in the Core Services, the Technical Support Services, the Additional Services, the Other related services, as well as all Diagnostic Data, Google writes that it may provide personal data "to our affiliates and other trusted businesses or persons to process it for us, based on our instructions and in compliance with our Privacy Policy and any other appropriate confidentiality and security measures. For example, we use service providers to help us with customer support."²⁸²

The fact that Google gives instructions to third parties (*other trusted businesses*) to process in compliance with (all 33 purposes of) the (consumer) Privacy Policy and appropriate confidentiality and security measures does not mean that Google has a (sub)processor agreement with these parties as referred to in Article 28 of the GDPR.

In sum, in the absence of an exhaustive list of specified and explicit purposes and the uncertainty about the amount of sub purposes Google may add, the collection of personal data through the G Suite Enterprise services does not comply with the principle of purpose limitation. As a result, government organisations cannot trust that Google will only process the personal data from G Suite Enterprise for legitimate purposes.

²⁸¹ Google, Affiliates providing business services in the EU, URL: https://privacy.google.com/businesses/affiliates/?hl=en_US

²⁸² Google (consumer) Privacy Policy, 'For external processing'.

14. Necessity and proportionality

14.1 The principle of proportionality

The concept of necessity is made up of two related principles, namely proportionality and subsidiarity. Personal data which are processed must be necessary for the purpose pursued by the processing activity. Proportionality means the invasion of privacy and the protection of the personal data of the data subjects is proportionate to the purposes of the processing. Subsidiarity means that the purposes of the processing cannot reasonably be achieved with other, less invasive means. If so, these alternatives have to be used.

Proportionality demands a balancing act between the interests of the data subject and the data controller. Proportionate data processing means that the amount of data processed is not excessive in relation to the purpose of the processing. If the purpose can be achieved by processing fewer personal data, then the data controller needs to limit the processing to personal data that are necessary.

Therefore data controllers may only process personal data that are necessary to achieve legitimate purpose. The application of the principle of proportionality is thus closely related to the principles of data protection from Article 5 GDPR.

14.2 Assessment of the proportionality

The key questions are: are the interests properly balanced? And, does the processing not go further than what is necessary?

To assess whether the processing is proportionate to the interests pursued by the data controller(s), the processing must first meet the principles of Article 5 of the GDPR. As legal conditions they have to be complied with in order to make the data protection legitimate.

Data must be '*processed lawfully, fairly and in a transparent manner in relation to the data subject*' (Article 5 (1) (a) GDPR). This means that data subjects must be informed about the processing of their data, that all the legal conditions for data processing are adhered to, and that the principle of proportionality is respected. As analysed in Sections 11.1 and 11.2 of this report, Google nor the government organisations currently have a legal ground for any of the processing through G Suite Enterprise. This means the personal data are not processed lawfully.

Google does not process the data in a transparent manner either. Google does publish extensive documentation for administrators about the 19 different audit log files they can access to monitor end user behaviour. However, at the time of completion of this DPIA Google did not publish documentation about other Diagnostic Data it collects through its own system-generated log files. The logs that can be accessed by admins do not contain any information about the website data Google collects, nor information about the use of Features, Additional Services, the Technical Support Services or the Other related services, or an exhaustive overview of all activities performed with a Google Account.

Google equally fails to provide any public explanation to its Enterprise customers in the EU about the other kinds of Diagnostic Data it collects through the use of the G Suite Enterprise services, such as the telemetry data. Administrators and end users cannot inspect the contents of these telemetry data either, nor does Google provide access thereto in response to a formal Data Subject Access request, as laid down in Article 15 of the GDPR.

The lack of transparency makes the data processing inherently unfair. The lack of transparency also makes it impossible to assess the proportionality of the processing.

The principles of data minimisation and privacy by design require that the processing of personal data be limited to what is necessary: the data must be '*adequate, relevant and limited to what is necessary for the purposes for which they are processed*' (Article 5(1)(c) of the GDPR). This means that the controller may not collect and store data which are not directly related to a legitimate purpose.

The principle of privacy by design (Article 25 (2) GDPR) requires that '*the data controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.*' According to this principle, the default settings for the data collection should be set in such a way as to minimise data collection by using the most privacy friendly settings.

As described in Section 3 of this report, Google frequently processes personal data in the Core Services with a privacy unfriendly default setting. This is the case for the accessibility of the Other related service Feedback.

Through Feedback, Google can process personal data in Customer Data for unauthorised purposes. In view of the possibly sensitive nature of such data, lack of transparency and possible risks for data subjects if Customer Data are processed for unlawful purposes and absence of opt-out controls, this processing is disproportionate.

Google equally fails to apply the principle of privacy by design with regard to data processing in the context of the Google Account, the Diagnostic Data, the Technical Support Services and the Additional Services.

Google frequently offers opt-out choices, instead of active opt-in choices. Google offers opt-out choices in many locations (different menus on the devices, in the browser and on different webpages). This places an unnecessary burden on the shoulders of the employees and makes the data processing disproportionate.

There is only one Google Account, that can be used in both an enterprise and consumer environment. All end users with a Google Account must accept the same general (consumer) Terms of Service and the (consumer) Privacy Policy, regardless if they create the account as a consumer or as an employee. Google explains that this is the case because end users may use their Google Account to sign into and use Google's consumer services, if their administrator does not restrict such use.

Google allows end users to sign-in with multiple Google Accounts. This design of the services does not sufficiently and systematically take the specific data protection risks for employees and the government organisations into account. Government organisations need to draw strict lines between processing of personal data in the consumer and enterprise environments, in order to prevent data breaches and unauthorised processing of personal data and Classified Information.

At the time of writing of this report, administrators could block access to the existing Additional Services for work accounts (not to any new Additional Services). However, they could not completely prevent logged in users from accessing Additional Services. When an end user accessed an Additional Service such a Google Search when logged-in with their work-Google Account, whilst the administrator had centrally disabled the use of the Additional Services, Google ensured that the user

was logged-out from the work account. Google then proceeded to process the data as if the user had not account at all.

This automatic (and privacy friendly procedure) does not apply to the use of all Additional Services. End users can for example use Google Photos with their enterprise Google Account. It is not clear why Google applies different rules to different Additional Services.

Google does protect the privacy of the work account when a government employee uses (the consumer service) Google Search. In that case, Google ensures that the data are processed as if the end user had no account. But this automatic procedure does not apply to the use of all Additional Services. Users can for example use Google Photos with their work credentials. It is not clear why Google applies different rules to different Additional Services.

The absence of a technical separation between enterprise and consumer Google Accounts, combined with the privacy unfriendly default setting of access to all Additional Services, leads to spill-over from personal data in Customer Data to Google's consumer environment. This is the case for (i) Ads Personalization, (ii) providing access to all Customer Data for the Chrome browser as 'trusted' app, (iii) the sending of telemetry data (Diagnostic Data) from Android devices, Chrome OS and the Chrome browser with data about app usage and use of biometric authentication, and (iv) installing three kinds of unique identifiers in ChromeOS and the Chrome browser and use these for installation tracking, tracking of promotional campaigns and field trials.

As long as these settings remain privacy unfriendly by default, and admins do not have controls to block or at least minimise the data processing with tools provided in G Suite Enterprise, the use of the Chrome OS, the Chrome browser and Android devices disproportionately infringes on the interests and rights of data subjects, in particular as regards confidential data or data of a sensitive nature or special categories of data. As joint controllers with Google, government organisations are accountable for the risks of any unlawful processing of personal data.

The principle of storage limitation requires that personal data should only be kept for as long as necessary for the purpose for which the data are processed. Data must *'not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data are processed'* (Article 5(1)(e), first sentence, GDPR). This principle therefore requires that personal data be deleted as soon as they are no longer necessary to achieve the purpose pursued by the controller. The text of this provision further clarifies that *'personal data may be kept longer in so far as the personal data are processed solely for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes in accordance with Article 89(1), subject to the implementation of appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject'* (Article 5(1)(e), second sentence, GDPR).

As explained in Section 10 of this report, Google will delete Customer Data actively deleted by the customer as soon as reasonably practicable, but can retain these data for half a year. This maximum period seems long, once a government organisation has decided to delete Customer Data.

With regard to the Diagnostic Data, the retention period of 6 months for most of the audit logs seems proportionate to the objectives pursued by admins, to be able to look back in case of data security incidents, and to regularly inspect the logs for correct application of the access rules.

Google does not have a fixed retention period for other types of Diagnostic Data, such as the telemetry and website data. The general rule is to retain these data for 6 months as well, but Google explained that “*other Diagnostic Data is retained for much longer periods (e.g. account deletion events).*”²⁸³ Cookie-based data are generally anonymized after 18 months, wrote Google. G Suite admins cannot customize these retention periods.

It is difficult to argue that 6 month old Diagnostic Data, or 18 months old data in the case of cookies, are necessary, adequate and relevant for the 22 or 33 purposes for which Google processes the Diagnostic Data as joint controller with the government organisations.

The processing of the Diagnostic Data through the Core Services and Additional Services, including the telemetry data and website data, does not meet the proportionality requirements. This is due to the lack of transparency, the privacy unfriendly default settings, the absence of technical opt-outs and the risk of unauthorised further processing of personal data in Customer Data by Google.

14.3 Assessment of the subsidiarity

When making an assessment of subsidiarity, the key question is whether government organisations can reach the same objectives (of using secure, bug free, modern communication and productivity software), with less intrusive means.

Google takes the view that end users of its G Suite Enterprise services voluntarily provide their consent to, or enter into a contract with, Google, (also) for the purpose of using consumer services. However, Google does not seem to take into account that the processing occurs in the context of an employment relationship. As assessed in Sections 11.2.1 and 11.2.2 of this report, employees are not free to give consent or enter into a contract with Google. There is no evidence that the specific contract with the data subject cannot be performed if the specific processing of the personal data in question does not occur. Reliance on either of these two legal grounds requires adequate purpose limitation to ensure that the personal data will not be processed for other purposes for which no legal grounds are available.

The consumer Terms of Service, and the (consumer) Privacy Policy apply to all the Additional Services (as well as Additional Product Terms), including the Chrome OS and the Chrome browser, to the use of the Google Account in these Additional Services and to all Diagnostic Data. These terms allow Google to process personal data for 33 broad purposes.

Government organisations can choose an alternative software provider and use a different browser. They can decide to use Microsoft Office 365 as an alternative, or open-source software. SLM Microsoft Rijk has published several DPIAs on Microsoft 365. Regardless of a choice for an alternative software provider, government organisations must identify the privacy and security risks of any software or cloud service they plan to use, and assess whether the software offers the necessary functionalities.

²⁸³ As quoted in Section 10.2. From responses provided by representatives of Google to SLM Microsoft Rijk during the course of this DPIA.

15. Data Subject Rights

This Section assesses whether government organisations and Google meet the GDPR requirements relating to data subjects rights and whether data subjects can effectively exercise such rights. Section 15.1 discusses the applicable GDPR framework and the arrangements in place between government organisations and Google. Sections 15.2 to 15.7 analyse whether data subjects can effectively exercise each of these rights.

15.1 Legal framework and contractual arrangements between government organisations and Google

The GDPR grants data subjects the right to information, access, rectification and erasure, object to profiling, data portability and file a complaint. It is the data controller's obligation to provide information and to duly and timely address these requests. If the data controller has engaged a data processor, the GDPR requires the data processing agreement to include that the data processor will assist the data controller in complying with data subject rights requests. In the event of joint controllership, the GDPR requires that the joint controllers '*shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them*'. The essence of the arrangement shall be made available to the data subjects.

As discussed in Section 5, government organisations and Google qualify as joint controllers for all processing in the context of G Suite Enterprise. This means that the arrangements with respect to data subjects rights and the provision of information should be agreed upon in a joint controller agreement as required by Article 26 GDPR. Such a specific joint controller agreement is not yet in place.

However, the G Suite DPA stipulates that Google will forward data subject rights requests with regard to Customer Data to the customer, and will provide assistance to the customer. Google explains that the customer will be responsible for responding to the data subject.

15.2 Right to information

Data subjects have a right to receive easily accessible, comprehensible and concise information about the processing of their personal data. This means that data controllers must provide data subjects with, *inter alia*, their identity as data controller, the purposes of the data processing, the intended duration of data storage and the data subjects' rights under the GDPR.

As explained in Sections 5 and above, government organisations and Google qualify as joint controllers and are therefore required to enter into a joint controller agreement. This agreement should include an arrangement with respect to their respective duties to provide data subjects with information. Currently, no such arrangement is in place.

As identified in Sections 3 and 4 of this report, Google does not provide government organisations or data subjects comprehensible information about the processing of personal data. Google does not provide a limitative list of purposes for the processing of Customer Data.

With regard to Customer Data in the Google Account (unless used in conjunction with a Core Service), the Additional Services, the Technical Support Services and the Other related services, as well as all Diagnostic Data, Google also fails to meet the

requirements for the quality and accessibility of information about the data processing. Although Google clearly tries to use plain language in its (consumer) Privacy Policy, the wording of the purposes is not explicit, and the explanations accompanying the purposes omit crucial information regarding what personal data will be processed for what specific purposes.

At the time of completion of this DPIA, Google did not publish documentation about the contents of the Diagnostic Data it collects on its own cloud servers (other than the audit logs it makes available for admins), nor about the contents of the telemetry data (Diagnostic Data) from ChromeOS, the Chrome browser, Android devices and apps.

As a result of the lack of information Google provides to government organisations, they are unable to provide data subjects adequate information about the processing of their personal data. The documentation published by Google also does not meet the standards set by the GDPR with regard to the right to information.

First of all, data subjects have a right to information. This means that data controllers must provide people with easily accessible, comprehensible and concise information in clear language about, inter alia, their identity as data controller, the purposes of the data processing, the intended duration of the storage and the rights of data subjects.

As has been highlighted in previous sections of this report, Google does not make comprehensible information available to data subjects about the processing of personal in the G Suite Enterprise Core Services. Quite the opposite. The G Suite DPA is the richest source of information, and this legal document requires enhanced close reading capacities. Google has refused to provide a limitative list of purposes for the processing of the Customer Data, insisting it only follows customer instructions.

With regard to all the Diagnostic Data, the Google Account Data, the Additional Services and related services such as Feedback, Google also fails to meet the requirements for the quality and accessibility of information about the data processing. Though Google clearly tries to use plain language in its Privacy Policy, the wording of the purposes is never explicit, and the explanations accompanying the purposes omit crucial information what personal data will be processed for what specific purposes.

Google does not publish documentation about the contents of the Diagnostic Data it collects on its own cloud servers, or about the contents of the telemetry data from the Chrome OS and browser, and Android devices.

As a result, the government organisations, as joint data controllers with Google, are unable to determine whether the processing is lawful in order to adequately inform their employees or students.

15.3 Right to access

Data subjects have a right to access their personal data. Upon request, data controllers must inform data subjects whether they are processing personal data about them. If this is the case, data subjects should be provided with a copy of such personal data, together with information about the purposes of processing, recipients to whom the data have been transmitted, the retention period(s), and information about their further rights as data subjects, such as filing a complaint with a Data Protection Authority.

As explained in Section 15.1, for data processing that falls in the scope of the G Suite DPA, Google undertakes to redirect access requests to its customers: *"If Google's Cloud Data Protection Team receives a request from a data subject in relation to Customer Personal Data, and the request identifies Customer, Google will advise the data subject to submit their request to Customer. Customer will be responsible for responding to any such request including, where necessary, by using the functionality of the Services."*²⁸⁴

Google provides administrators access to 19 audit log files (Diagnostic Data). These audit log files do not provide a complete overview of all personal data processed by Google about the use of all Core Services and the Google Account. Google also does not provide access to the website and cookie data it collects in the Core Services (Diagnostic Data), or other data such as Support Data, data about the use of the Features and embedded Additional Services such as Maps in the Core Services. As described in Section 1.4.1, different types of Features were used in the test scenarios and underwater traffic to Maps was observed in the intercepted internet traffic evidencing that Google processes such data.

As data controller, Google has pointed to some tools where end users can see some of their usage data. However, Google did not provide the requested overview of all personal data processed by Google in its Additional Services, nor the Diagnostic Data resulting from the use of the Core Services and the Additional Services. Google acknowledges in its reply to the access requests made in the context of this DPIA that some data, such as cookie identifiers, are personal data, but Google states it cannot reliably verify that the person making the data subject access request is the data subject that these data relate to. Google did not accept the offer from the researchers to receive additional information enabling their identification.

This refusal is problematic in view of Article 11 (2) of the GDPR. This provision states: *"Where, in cases referred to in paragraph 1 of this Article, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 15 to 20 shall not apply **except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification.**"*

Google did not demonstrate that it is not in a position to identify the data subject in the context of the access requests of this DPIA. Since the researchers created the Google Accounts specifically for test purposes, using their real identity, on clean test devices, there is no possibility that the device or user identifiers belonged to another individual or could be confused with other data subjects.

As Recital 57 of the GDPR explains: *"the controller should not refuse to take additional information provided by the data subject in order to support the exercise of his or her rights. Identification should include the digital identification of a data subject, for example through authentication mechanism such as the same credentials, used by the data subject to log-in to the on-line service offered by the data controller."*

If Google is able to use the digital credentials of an end user to reliably provide access to the most sensitive content data stored in a user's Drive or Gmail account, it is not comprehensible why Google would not be able to provide access to Diagnostic Data based on those same credentials, possibly combined with information only an end user can access on his or her own device.

²⁸⁴ Clause 9.2 G Suite DPA.

Google is able to create billions of dollars of value in personalised advertising based on Diagnostic Data. This requires a technical capability to track individual behaviour over time and across services. The large scope of the processing operations means that data subjects can expect more effort from Google to provide meaningful access to personal data.

In sum, when a data subject exercises his or her rights under the GDPR and requests access to the personal data that Google processes, he or she can only access personal data in the audit logs about the use of some Core Services via the administrators of the government organisation, and view a limited amount of personal data through end user tools. This is not a complete overview of all personal data processed by Google.

Where Google and the Dutch government organisations are joint controllers for the G Suite Enterprise services, they must agree upon effective arrangements through which data subjects can exercise their rights. Although the G Suite DPA does provide some information with respect to the exercise of data subjects rights, the proposed procedure is not effective as data subjects do not obtain an overview of all personal data.

15.4 Right of rectification and erasure

Data subjects have the right to have inaccurate or outdated personal data corrected, incomplete personal data completed and - under certain circumstances - personal data deleted or the processing of personal data restricted. At present, neither Google nor the government organisations can actually delete historical Diagnostic Data, except for completely the Google Account on the domain of the customer.

According to Google, it is not possible to delete individual historical Diagnostic Data, because: *"Our technical infrastructure that performs log anonymization and deletion is not designed to have direct access to information identifying the customer. All retention is governed by the retention rule provided by Google engineering when configuring each multi-tenant log."*

Additionally, as quoted in Section 10, Google *in general* does not retain Diagnostic Data for longer than 180 days, but Diagnostic Data about deleted Google Accounts are kept *for much longer periods*.

It is questionable whether this design and this retention policy meet the requirements of Article 17(1)(a) and Article 17(1)(d) of the GDPR of the GDPR. These provisions require a data controller to delete personal data *without undue delay* upon request of a data subject if they are no longer needed for the purposes for which they were collected or otherwise processed, or when the personal data have been unlawfully processed.

15.5 Right to object to profiling

Data subjects have the right to object to an exclusively automated decision if it has legal effects. As explained in Section 11.2 of this report, as joint controllers with Google, government organisations do not have a legal ground for the processing of personal data from employees or other data subjects for personalized advertising purposes. It is not necessary therefore to explore if such processing would be profiling.

When Google processes personal data from the G Suite Core Services, there are no known decisions that Google makes that have legal consequences or other noteworthy consequences for the rights and freedoms of the data subject. Therefore, this specific right of objection does not apply in this case.

15.6 Right to data portability

Data subjects have a right to data portability if the processing of their personal data is carried out by automated means and is based on their consent or on the necessity of a contract. As explained in Sections 11.1 and 11.2 of this report, the processing by government organisations and Google cannot be based on either of these legal grounds.

The individual right to data portability is independent of the situation where government organisations themselves would have to move their processing and files collectively to another provider. Google recognises this collective right to portability and has started the Data Transfer Project. Facebook, Microsoft, Apple and Twitter are participating in this initiative.²⁸⁵

15.7 Right to file a complaint

Finally, government organisations as (joint) controllers must inform their employees about their right to complain, internally to their Data Protection Officer (DPO), and externally, to the Dutch Data Protection Authority (Autoriteit Persoonsgegevens).

In sum, neither Google, nor the government organisations are currently in a position to (fully) honour the rights of data subjects.

²⁸⁵ Data Transfer Project, URL: <https://datatransferproject.dev/>

Part C. Discussion and Assessment of the Risks

This part of the DPIA contains a discussion and assessment of data protection risks relating to the use of G Suite Enterprise. This part starts with an overall identification of the risks in relation to the rights and freedoms of data subjects, resulting from the processing of information about their use of, and behaviour in, the G Suite Enterprise services.

This Part C starts with an overall identification of the risks in relation to the rights and freedoms of data subjects resulting from the processing of their personal data in the context of the G Suite Enterprise services.

Part D of this DPIA provides an analysis of mitigating measures for the identified risks.

16. Risks

16.1 Identification of Risks

The processing of personal data about the individual use of the G Suite Enterprise Core Services and the Additional Services (including the Chrome OS and browser), in combination with the built-in Features and Other related services such as Feedback, results in two types of general risks. First, risks through the processing of Diagnostic Data about the use of the services and the installed apps, and secondly, risks resulting from the processing of Customer Data.

16.1.1 *Metadata (Diagnostic Data)*

As explained in Section 1.2, the G Suite Enterprise services include the collection of different types of Diagnostic Data.

Google and the government organisations have access to audit log files that contain Diagnostic Data about end user behaviour. These log files can potentially be used to create a profile of the G Suite end users. The audit log files contain information about the use of the different G Suite applications and contain the detailed activity overviews. The log files provide information about the individual log-in behaviour, email behaviour and service usage. Government organisations could potentially use these data for a negative performance assessment of an employee, if such usage were not explicitly excluded, or at least limited to exceptional circumstances, by internal data protection policy rules.

Government employees may also feel unable to exercise their right to (moderately) make use of government facilities without being observed and to communicate about private affairs, such as sending an email to a friend or family member.

Google collects detailed Diagnostic Data about end user behaviour in (for example) the Core and Additional Services. As explained in Section 2.3 of this report, Google collects more Diagnostic Data on its cloud servers than admins can see in the available audit logs, such as Diagnostic Data relating to the use of the Features and to Technical Support Services Requests.

Google frequently uses settings that maximise the data processing by default, instead of minimising it. The Additional Services for example, are all enabled by default for G Suite Enterprise customers. Google also collects Diagnostic Data about G Suite app usage and the use of biometric authentication through telemetry data from the (Additional Service) Chrome OS and the Chrome browser, and from Android devices. It is not clear what Diagnostic Data Google exactly collects about the use of its Additional Services and the Google Account.

Google qualifies itself as the data controller for Diagnostic data (including the telemetry and website data). Google permits itself to process the Diagnostic Data for at least 33 distinct purposes in its (consumer) Privacy Policy, plus additional specific purposes for the processing via Chrome OS and the Chrome browser. Due to the default settings, there is a clear interdependency between the Core Services and the Additional Services. Google finds that it may process the contents and the Diagnostic Data about the use of the Additional Services, including the Google Account Data, and Other related services as an independent data controller. This is incorrect.

The above leads to multiple data protection risks, as Google:

- does not provide a limitative list of purposes for which it processes Diagnostic Data;
- is not transparent about the Diagnostic Data it collects (from either the Core Services, the Features, the Google Account, the Additional Services, the Technical Support Services and the Other Related Services);
- does not provide controls to administrators or end users to block or limit the collection of Diagnostic Data; and
- refuses to provide access to all Diagnostic Data pursuant to formal data subject access requests.

If such Diagnostic Data are accessed unlawfully, there is a risk of blackmailing and stalking of employees or other data subjects based on such data. Government employees may be inhibited from exercising their legitimate rights, or feel unable to exercise their right to whistle blow. The knowledge that the government organisations can process these Diagnostic Data for profiling purposes can cause a *chilling effect* on employees and other licensed government users of the G Suite Enterprise services. A chilling effect is the feeling of pressure someone can experience through the monitoring of his or her behavioural data, discouraging this person from exercising their rights, such as accessing certain content.²⁸⁶

Note: Changes made by Google after completion of this DPIA report are described in the new assessment of the risks added to the summary and conclusion of this report in February 2021.

16.1.2

Content (Customer Data and content collected through Diagnostic Data)

Google collects and processes content that is included in Customer Data in different ways. For example, Google receives every character a user enters and stores in online text, collaboration, presentation, calculation and other tools and services. Content may also be included in Support Data and provided to Google in the context of the Google Account. As explained in Section 2.5.1 of this report, the Customer Data may include sensitive or Classified Information, and sensitive and special categories of personal data of many categories of data subjects, not just government employees. The file and path names may reveal Classified Information or otherwise sensitive or confidential government materials.

²⁸⁶ Merriam-Webster Online Dictionary, "chilling effect", URL: https://www.merriam-webster.com/legal/chilling_effect.

The Diagnostic Data collected by Google contain content from data that Google obtains as Customer Data in two different ways.

First, Google collects content from Customer Data such as files, emails or chats when a data subject uses a Feature, such as *Spelling and Grammar*.

Second, Google collects content from data that Google obtains as Customer Data such as file and path names of documents in its Diagnostic Data, and snippets of content in telemetry data from the *Enhanced Spellchecker*.

There are multiple risks related to the possible further processing of these Customer Data and content from Customer Data collected through Diagnostic Data by Google. Google permits itself to process personal data in Customer Data for 8 and perhaps 20 purposes. As explained in Section 5.2, Google does not qualify as a data processor for the processing of Customer Data due to the lack of transparency about the purposes, lack of purpose limitation and the fact that Google determines compatible purposes of use.

Additionally, Customer Data may be included in Diagnostic Data. Diagnostic Data may contain Confidential Information or organisation data of a potentially sensitive nature, such as files names and subject lines of email, sentences and words if the *Spelling and grammar* is used, and sensitive or special categories of personal data of all kinds of data subjects. Such Diagnostic Data do not fall within the scope of the G Suite DPA. This means, *inter alia*, that third parties engaged by Google that receive these data are not authorised as subprocessors, and are not bound by G Suite DPA (and potentially also not by the GDPR).

Furthermore, where government organisations and Google are joint controllers for Diagnostic Data that includes (content) data obtained by Google as Customer Data, government organisations generally do not have a legal ground for such processing, because it will mostly not be necessary to process such data.

There is a risk that Google may be ordered by a foreign government to hand over Customer Data or Diagnostic Data from Dutch government customers. Google may be prohibited from forwarding such a request to the government organisation and may also be prohibited from even informing the organisations thereof by a gagging order. Customer Data and Diagnostic Data may also be accessed unlawfully by a rogue administrator or hostile state actor. Such access would be in breach of confidentiality requirements and the fundamental right to protection of communication secrecy.

16.2 Assessment of Risks

The risks can be grouped in the following categories:

1. Loss of control over the processing of personal data;
2. Loss of confidentiality;
3. Inability to exercise fundamental rights (GDPR data subject rights as well as related rights, such as the fundamental right to send and receive information);
4. Reidentification of pseudonymised data; and
5. Unlawful (further) processing.

These risks have to be assessed against the likelihood of their occurrence and the severity of their impact.

The UK data protection commission ICO provides the following guidance regarding the assessment of risks:

*"Harm does not have to be inevitable to qualify as a risk or a high risk. It must be more than remote, but any significant possibility of very serious harm may still be enough to qualify as a high risk. Equally, a high probability of widespread but more minor harm might still count as high risk."*²⁸⁷

This report therefore assesses a list of specific risks, under the specific circumstances of the investigated data processing.

16.2.1 *Lack of purpose limitation Customer Data*

Google does not provide a limitative list of the purposes for which it processes the personal data in Customer Data from its Core Services, including the embedded Features such as *Spelling and Grammar*. Google insists it only processes personal data following its customer's instructions. The only purpose explicitly included in the instructions in the G Suite DPA is to provide the Core Services and the Technical Support Services. This DPIA shows that Google factually processes the Customer Data for at least 6 purposes. Additionally, Customer Data may be processed for 12 other purposes which are mentioned in Google's General Privacy Policy as examples of 'providing the service'.

Some of these purposes are predictable and may be necessary to provide the G Suite Enterprise services to the government organisation. However, other purposes can lead to surprises. This is for example the case with the reuse of Customer Data from the Feature *Spelling and grammar* to improve the service for customers with machine learning.²⁸⁸

As explained in Section 5.3, Google qualifies itself as an independent data controller data for the processing of personal data in the Google Account when used outside of the Core Services, the Additional Services, Other related services such as Feedback and for all Diagnostic Data. Google permits itself to process such data for 33 purposes mentioned in its General Privacy Policy. These purposes are generally aimed at serving Google's own commercial interests. Google does not explain what personal data it uses for what purposes and only provides some examples. This allows Google to dynamically add or stop collecting Customer Data for any of these purposes.

Customer Data can include confidential or Classified Information, and sensitive and special categories of personal data of all kinds of data subjects, not just government employees.

Google has explained it applies anonymisation techniques to personal data. One of the techniques mentioned by Google is '*sampling to create aggregate data*'. If Google acts a data processor for the processing of personal data in Customer Data, Google may only process personal data for creating aggregated data for analytical purposes if the customer explicitly instructs Google to do so. If Google decides on its own initiative to process Customer Data for its own analytical purposes, there is a risk of a loss of confidentiality and unlawful further processing of Customer Data.

Due to the lack of specific and explicit purposes for the processing of personal data in Customer Data, the likelihood is high that Google unlawfully processes Customer Data because (i) those purposes are not part of the documented instructions of

²⁸⁷ ICO, How do we do a DPIA?, URL: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/>.

²⁸⁸ After completion of this DPIA, Google provided the guarantee that it will only use content data for this type of machine learning within a customer's domain.

customer or (ii) Google incorrectly assumes it has the liberty to process these Customer Data for its own (commercial) purposes.

As a result, the risk of unlawful processing is likely. This can have a serious impact for the data subjects, for example because Google can use their personal data for customised contents or marketing. The privacy risks for the data subjects are therefore high.

16.2.2 *Lack of purpose limitation Diagnostic Data*

Google qualifies itself as data controller for all Diagnostic Data, regardless of its origin in the use of the Google Account, the Core Services, the Additional Services, related services such as Feedback or the Technical Support Services. Google incorrectly assumes it therefore has the liberty to process these Diagnostic Data for all 33 purposes in its General Privacy Policy. At the time of the completion of this report, Google did not provide additional information about the purposes. On 12 November 2020 Google published a list of 17 purposes for the Diagnostic Data in the Google Cloud Privacy Notice.²⁸⁹

Due to the lack of specific and explicit purposes in the General Privacy Policy the likelihood is high that Google processes the Diagnostic Data unlawfully.

Diagnostic Data can include a wide range of personal data, such as personal data in Customer Data, detailed information about individual G Suite end user activities in the G Suite Core and Additional Services, file and path names originating from Customer Data, unique end user and device information, including IP address and hashed MAC address, information about app usage and use of biometric authentication, with timestamps, crash reports, and, in Chrome OS and the Chrome browser, three unique tracking identifiers.

In view of the sensitive nature of the Diagnostic Data, the lack of purpose limitation and the impossibility to prevent Google from collecting these data, the likelihood of unlawful processing is high, while the negative consequences may have a serious impact. Therefore, this results in a high data protection risk.

16.2.3 *Lack of transparency Diagnostic Data*

Though Google publishes documentation for administrators about the 19 different audit log files they can access to monitor end user behaviour, Google does not provide any public explanation to its customers about the other kinds of Diagnostic Data it collects through the use of the G Suite Core Services. Google also does not clearly communicate to customers that Diagnostic Data do not constitute personal data in Customer Data and therefore fall outside of the scope of the G Suite DPA.

Google collects more Diagnostic Data on its cloud servers than admins can see in the available audit logs, such as use of the built-in Features or Diagnostic Data about Technical Support Requests. The lack of public documentation means that data subjects do not have sufficient insight into what information is recorded about their behaviour. Google also does not provide full access to these Diagnostic Data to G Suite Enterprise admins, or to data subjects pursuant to data subject access requests. Data subjects therefore cannot effectively exercise their fundamental right to access their personal data. This risk is addressed separately below, in Section 16.2.10 of this report.

Google incorrectly considers all information about the collection of telemetry data confidential (part of the Diagnostic Data). Google only provides one opaque sentence

²⁸⁹ Google, Google Cloud Privacy Notice, 7 December 2020, URL: <https://cloud.google.com/terms/cloud-privacy-notice>

in its (consumer) Privacy Policy, and a list of telemetry events (atoms) in a specialised source for Android developers, but does not provide specific information to G Suite Enterprise end users or admins. Google explains: *"We also collect information about the interaction of your apps, browsers, and devices with our services, including IP address, crash reports, system activity, and the date, time, and referrer URL of your request."* Google does not publish any documentation about the specific data it collects through telemetry. Because the outgoing traffic from the G Suite apps and Chrome browser is encrypted, and Google does not offer a tool to decrypt the traffic, end users and admins cannot access the contents of the telemetry data (Diagnostic Data).

In its investigation of the telemetry data that Google collects, Privacy Company has observed the presence of personal data and sensitive Customer Data (in the Enhanced Spellchecker and in telemetry data about app usage). Privacy Company has to assume that some, if not all telemetry data contain (1) personal data in the form of unique end user and device information, including IP address and hashed MAC address (2) information about app usage and use of biometric authentication, with timestamps, (3) crash reports, (4) three unique tracking identifiers and (5) sometimes very sensitive Customer Data.

Google also collects Diagnostic Data in the form of website data, with the help of cookies or similar technologies. In its (consumer) Privacy Policy Google writes:

"We collect information about the apps, browsers, and devices you use to access Google services (...) The information we collect includes unique identifiers, browser type and settings, device type and settings, operating system, mobile network information including carrier name and phone number, and application version number."

Google does not inform G Suite Enterprise end users that Google DoubleClick collects data when a non-authenticated end user visits a login page for the G Suite Core Enterprise services. According to Google this is necessary to check a user's Ads Personalization preferences. Google does not provide this information in its public documentation about cookies (in its (consumer) Privacy Policy).

The lack of access to the contents of Diagnostic Data, combined with the absence of any detailed public documentation what specific personal data are processed for what purposes, results in the fact that data subjects cannot know what personal data Google collects about their behaviour. Moreover, because Google does not explain what personal data it collects for what purposes, there is a risk that Google silently changes the data collection, without informing data subjects or admins.

The consequences for data subjects of this lack of transparency are serious. As Recital 58 of the GDPR explains: *"This [transparency] is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising."*

Due to the lack of transparency, there is a high risk that it is impossible for data subjects to exercise their data subject rights. Moreover, there is a non-negligible chance of loss of confidentiality, re-identification of pseudonymised data and unlawful (further) processing if these Diagnostic Data are stored as pseudonymised data in Google's central log repository. Given the nature of the Diagnostic Data, the consequences for data subjects can be serious. Therefore, the lack of transparency about the Diagnostic Data leads to a high risk for data subjects.

At the moment of completion of this DPIA, Google announced, in reply to this DPIA, that it would create an Enterprise Privacy Notice with information about the Diagnostic Data. In December 2020, after completion of this DPIA, Google published the Google Workspace Data Protection Implementation Guide.²⁹⁰

16.2.4 *Lack of transparency Customer Data*

As explained in Section 16.2.3 above, Google also processes Customer Data as part of Diagnostic Data. This is for example the case in system-generated server logs on Google's cloud servers. The Drive audit log for example shows that Google processes Customer Data such as the file and path names of documents (*Item name*), user and account names, email addresses as well as IP addresses as Diagnostic Data.

Google can also collect Customer Data via telemetry data from the Chrome browser, as well as contents that may be included in crash reports sent through the telemetry clients in the installed apps, and Customer Data that are sent by end users in Technical Support Requests. It follows from the intercepted data traffic that Google also collects words and sentences from documents through telemetry if an end user uses the Chrome *Enhanced Spellchecker*.

Google does not provide clear and centrally accessible information about the processing of Customer Data as part of Diagnostic Data.

Google similarly does not provide information about, or access to, the Diagnostic Data from its Additional Services. It is not unlikely that Google collects some contents of files, emails or chats in Diagnostic Data when an end user uses an Additional Service such as Google Groups, Classroom, Photos or as keywords in Google Alerts.

Google serves a Welcome notice to every new G Suite Enterprise end user. This Welcome notice contains hyperlinks to various sources of information and ends with references to the consumer Terms of Service and (consumer) Privacy Policy. Users have to click 'Accept' to continue with their Google Account creation. After clicking 'Accept', the notice disappears, and the information is no longer accessible. This practice does not comply with the GDPR requirements for transparency.

In replies to questions about the processing of content that is part of Customer Data via the Features *Spelling and grammar*, *Translate* and *Explore*, Google explained that it processes these data in the same way as personal data in Customer Data from the Core Services. Google has not published any information about these Features, and the processing thereof is not explicitly covered in the G Suite DPA.

Google also does not inform end users in a clear and transparent way that it offers three different kinds of spelling checker. One as Feature in the Core Services (*Spelling and Grammar*), and two in the Chrome browser (*Basic Spellchecker* and *Enhanced Spellchecker*). For end users, the difference is not clear, as all three of these spellcheckers can be accessed in Docs, when accessed with the Chrome browser. Google does not explain that use of the *Enhanced Spellchecker* means that it will collect contents of documents as part of the telemetry data stream for Diagnostic Data.

In the Core Services, end users can access a 'Feedback' module. This functionality invites the end user to send a screenshot to Google, but the end user can also provide free text. In the text box, Google mentions that it can use the data to improve its

²⁹⁰ Google Workspace Data Protection Implementation Guide, URL https://services.google.com/fh/files/misc/google_workspace_data_protection_guide_en_dec2020.pdf

services and refers to its (consumer) Privacy Policy. Google does not warn users clearly enough that this means Google can process submitted data (that may include Customer Data) for all 33 purposes of its General Privacy Policy.

The lack of transparency leads to a high likelihood that risks occur such as loss of control, loss of confidentiality and unlawful further processing. In view of the sensitive nature of the Customer Data, the consequences for data subjects can be serious. Therefore, the lack of transparency about the Customer Data leads to a high risk for data subjects.

16.2.5 No legal ground for Google and government organisations as joint controllers without agreement

As explained in Chapters 4 and 13 of this report, the processing of personal data in the context of the G Suite Enterprise services currently does not comply with the principle of purpose limitation. With regard to personal data in Customer Data from the Core Services, and according to Google also the Features and Google Account when used in conjunction with a Core Service,²⁹¹ the G Suite DPA does include a general purpose. This purpose is too broad and therefore not specific. This DPIA shows that Google factually processes Customer Data for 6 or perhaps 20 purposes. Without a specific purpose or specific purposes, it is impossible for government organisations to identify any appropriate legal ground that allows them to process personal data.

Where Google is a joint controller, the purposes of the processing are included in its (consumer) Privacy Policy. This Privacy Policy lists non-limitative, list of purposes that are not specific, nor explicit. As such, specific purposes for processing are unknown of the Additional Services, the Google Account (when not used in conjunction with a Google Account), the Technical Support Services and the Other related services, as well as all Diagnostic Data. Without a specific purpose or specific purposes, it is impossible to identify any appropriate legal ground that Google can invoke for processing of personal data.

Detailed analysis of the four possible legal grounds for the data processing (consent, contract, public interest and legitimate interest) shows that the government organisations do not have a legal ground for the processing of any personal data in, about and related to the use of G Suite Enterprise.

The lack of any legal ground makes the data processing unlawful, and leads to loss of control over the personal data of data subjects (employees and other data subjects that communicate with the Dutch government). The likelihood of occurrence of this risk is 100% in the current circumstances, while the impact on data subjects of the processing of their personal data for Google's 33 purposes, is serious. This leads to a high risk for data subjects.

16.2.6 Missing privacy controls for admins and data subjects

Some of the data protection risks caused by the lack of purpose limitation and lack of transparency about the data processing could be mitigated if admins had central access to privacy controls limiting or blocking certain data processing.

Though Google does offer some controls to admins and end users, there are no central controls for admins to:

1. Prevent use of *Enhanced Spellchecker* in the Chrome browser. This can only be done by buying an extra license for each end user in Chrome Enterprise(out of scope of this DPIA)

²⁹¹ See Sections 1.4.2 and 1.4.3 of this report.

2. Prevent reuse of spelling data for machine learning by Google.²⁹²
3. Limit the collection of telemetry data (Diagnostic Data);
4. Change the default setting for Ads Personalization to Off²⁹³;
5. Prohibit the use of data controller services such as Feedback in the Core Services.

The lack of privacy controls to limit the data processing can lead to a loss of control, loss of confidentiality and unlawful further processing. In view of the potentially sensitive nature of the Customer Data, as may also be included in telemetry data (Diagnostic Data) and in screenshots provided through Feedback, the consequences for data subjects can be serious. Therefore, the lack of privacy controls leads to a high risk for data subjects.

16.2.7 *Privacy unfriendly default settings*

The use of some privacy unfriendly default settings in G Suite Enterprise and the Chrome browser can lead to additional data protection risks for government employees.

This is the case for the use of the Additional Services. The Additional Services are enabled by default in G Suite Enterprise. Google explains that it has chosen this setting *"to offer a smooth experience to G Suite customers, with no additional charge."*²⁹⁴

As explained in Section 3.1.6, Google has also switched *Ads Personalization On* by default. This design choice colours the statement 'without additional charge' for the Additional Services. In the G Suite DPA, Google promises it will not use Customer Data from the Core Services for personalized advertising, or show advertising in the Core Services. However, Google does have an interest in monetizing personal data from and about the use of the Additional Services through behavioural advertising. This goal is best served by turning Ads Personalization On. Additionally, Google does not allow admins to centrally change this default setting.

As explained in Section 3.2.3, end users have access to all Marketplace apps by default. By default, all installed Marketplace apps have unrestricted access to Customer Data. Administrators have three choices in managing the G Suite Marketplace: they can prohibit the installation of all apps, allow only whitelisted apps, or allow all apps.

Google's Chrome browser also has a number of privacy unfriendly default settings. Google considers the use of Chrome entirely optional: *"Chrome Browser and Chrome OS are each consumer products, and are optional ways to access G Suite."*²⁹⁵

The Chrome browser has access to the Google Account and all Customer Data by default, as Google considers this a trusted app. Administrators can only disable this access if they buy the separate Chrome Enterprise product, not included in the G Suite Enterprise offering, and therefore out of scope of this DPIA.

Chrome OS and the Chrome browser by default install three kinds of unique identifiers and use these for:

²⁹² In reply to this DPIA, Google provided guarantees that machine learning based on Customer Data for spelling and grammar are restricted to the relevant customer account.

²⁹³ In reply to this DPIA, Google will turn this setting to default off for new users.

²⁹⁴ Google reply to part A of the DPIA. After completion of this DPIA, Google has provided controls for admins to block access to the Additional Services from work accounts.

²⁹⁵ Idem.

- Installation tracking
- Tracking of promotional campaigns
- Field trials

Admins cannot block the use of these unique identifiers. The three purposes for which Google processes these unique identifiers are commercial. If used in combination with G Suite Enterprise, the Chrome browser thus 'leaks' data from the enterprise environment to the consumer environment. The word 'Field trials' could refer to the delayed introduction of new features and services, but could also mean A/B testing on customer groups. Because there are no granular controls for admins per purpose, the combined purposes lead to a loss of control over the processing of personal data.

Privacy unfriendly default settings do not comply with the privacy by default and design principles in Article 25 from the GDPR. With such default settings Google benefits from cognitive biases that prevent admins and end users from making any changes to the default settings, even if those settings are not aligned with their privacy interests. This may lead to a loss of control. Personal data of data subjects may be used for profiling and behavioural advertising. This may lead to serious adverse consequences for data subjects. Therefore, the use of privacy unfriendly default settings leads to a high risk for data subjects.

16.2.8

One Google Account

As explained in Section 1.4.2, Google does not provide separate Google Accounts for the consumer and enterprise environments. Google separates its G Suite Enterprise services from its consumer services per service, not per user. This design choice can lead to spill-over of personal data from the G Suite enterprise environment to the consumer environment.

As explained in Section 1.4.3, this is for example the case when a G Suite Enterprise end user has to install the Device Policy app from Google's Play Store. Administrators have no choice but allow the use the Google Play Store as an Additional Service to be able to install the Device Policy App. Employees frequently have no real choice either; either because they have already bought an expensive Android device and need to have it managed as Bring Your Own Device, or because their employer has centrally procured or provides corporate Android devices.

Google has made a design choice to allow end users to sign-in with multiple Google Accounts. Google explains in a help page: "*When you're signed in with more than 1 Google Account at the same time, ads may be based on ad settings for your default account. Your default account is usually the account you signed in with first.*"²⁹⁶ This could lead to spill-over from the enterprise to the consumer environment. This can for example be the case where an employee is simultaneously logged-in with his work-related Google Account and his consumer Google Account and uses Google Search while the administrator has centrally switched *Off* the use of the Additional Services, including Google Search.

In that case, when the end user accesses Google Search, he is automatically treated as though he would not have a Google Account. As a result, the user may see Ads based on the relevant browsing session. However, because that user is also logged in with another Google Account, Google may take into account the contents of and metadata about the relevant search queries for Ads Personalisation of the consumer Google Account. The employee is unaware of this, because Google does not show a warning that the employee is leaving the protected enterprise environment.

²⁹⁶ Google, Control the ads you see, URL: <https://support.google.com/ads/answer/2662856>.

As recently recalled by the EDPS, "*Big Data Comes comes with big responsibility and therefore appropriate data protection safeguards must be in place and effectively applied.*"²⁹⁷ Google can mitigate the risks of its design choice for one Google Account by either preventing multiple log-ins, or by offering a clear protection against further processing. In both circumstances, end users need to be alerted.

There is a reasonable possibility that employees sign-in with multiple Google Accounts. The spill-over from the enterprise to the consumer environment can lead to serious negative consequences for data subjects, because Google can use content data from the enterprise environment for Ads Personalization and all other purposes from its (consumer) Privacy Policy. Therefore, the privacy risks for data subjects are high.

16.2.9 *Lack of control over subprocessors Customer Data and Diagnostic Data*

In the G Suite DPA and in responses to this DPIA, Google explains that it uses subprocessors to process Technical Support Services requests. These requests may include Customer Data. Google has explained it applies 4 types of security safeguards to limit subprocessors' access to Support Data. Google verifies compliance with the information security requirements through annual audits. Google has also provided a limitative list of subprocessors who may provide support in English or Dutch to Dutch government organisations. Additionally, Google has presented some of the contents of data processing agreements with its subprocessors to the external law firm engaged by SLM Microsoft Rijk.

Despite these measures, Google's procedure to engage subprocessors does not give government organisations sufficient control over the processing of employee personal data. As explained in Section 5.3.6, customers must have meaningful control over the engagement of subprocessors by Google and the processing of personal data by such subprocessors. Google allows customers to object to the engagement of new subprocessors. However, customers cannot exercise meaningful control over the engagement of new subprocessors as customers can only object by terminating the agreement. Terminating the agreement as sole and exclusive remedy can deter data controllers from objecting to new subprocessors as the consequences of termination are far-reaching. Google therefore effectively decides which third parties engaged as new subprocessors may have access to personal data without giving meaningful control thereof to its customer.

Diagnostic Data

There are also risks for data subjects where Google engages other third parties to process Diagnostic Data, especially because this DPIA identified that Google also collects Diagnostic Data that contains content from files that are obtained by Google as Customer Data. In its General Privacy Policy, Google does not offer adequate information about such third parties: "*We provide personal information to our affiliates and other trusted businesses or persons to process it for us, based on our instructions and in compliance with our Privacy Policy and any other appropriate confidentiality and security measures. For example, we use service providers to help us with customer support.*" Government organisations currently have no control over which third parties process Diagnostic Data as the processing of Diagnostic Data falls outside of the scope of the G Suite DPA.

²⁹⁷ The European Data Protection Supervisor ('EDPS'), Opinion 3/2020 on the European strategy for data, 16 June 2020, par. 75, URL: https://edps.europa.eu/sites/edp/files/publication/20-06-16_opinion_data_strategy_en.pdf

Customers have no meaningful control in the G Suite DPA regarding the engagement of new subprocessors by Google for the processing of Customer Data. The loss of control over subprocessing can lead to negative consequences for data subjects. A customer may wish to object to a new subprocessor engaged by Google, but may withhold such objection as it would have to terminate the agreement. Customers also have no control over third parties that are engaged by Google for the processing of Diagnostic Data as the processing of Diagnostic Data falls outside of the scope of the G Suite DPA. Therefore, the privacy risks for data subjects are high.

16.2.10 Inability to exercise data subjects access rights

In response to two data subject access requests, Google did not provide the requested overview of all personal data it processes as a data controller. This should have included the personal data it processes as data controller, but that are not made available to administrators. The overview should have also included all the Diagnostic Data resulting from the use of the Core and the Additional Services, use of the Additional Services and use of ChromeOS and the Chrome browser.

Google acknowledges in its reply to the access requests that some data, such as cookie identifiers, are personal data, but Google states it cannot reliably verify that the person making the data subject access request is the data subject that these data relate to. Google was not willing to let the researchers provide additional information enabling their identification. Since the researchers created the Google Accounts specifically for test purposes, using their real identity, on clean test devices, there is no possibility at all that the device or end user identifiers belonged to another individual or could be confused with other data subjects.

If Google is able to use the digital credentials of an end user to reliably provide access to the most sensitive content data stored in a user's Drive or Gmail, it is not comprehensible why Google would not be able to provide access to Diagnostic Data based on those same credentials, possibly combined with information only an end user can access on his or her own device.

Google is able to create billions of dollars of value in personalised advertising based on Diagnostic Data. This requires a technical capability to track individual behaviour over time and across services. The large scope of the processing operations means that data subjects can expect more effort from Google to provide meaningful access to personal data.

The impossibility for data subjects to exercise their fundamental privacy rights per definition leads to a high risk. The probability that this risk occurs, is 100%, as Google is not willing to let data subjects provide additional information enabling their identification. That is why the privacy risks for data subjects are high.

16.2.11 Cloud provider: unlawful access to Customer Data and Diagnostic Data

As explained in Section 7 of this report, the transfer of personal data to outside of the EEA poses a risk in itself, because the standard of protection of personal data in most countries in the world is lower than in the European Union. Section 12.1 describes three general risks for unlawful further processing of personal data:

- (i) through orders to Google from US law enforcement authorities, security agencies and secret services;
- (ii) by rogue administrators at Google and at subprocessors; and
- (iii) by hostile state actors.

Google takes a number of different technical and organisational measures to protect personal data against the risks of rogue administrators and against attacks from hostile state actors. Google also encrypts all Customer Data on disks and backup

media and in transit. Google stores the encrypted data in smart chunks with rotating keys. These measures all contribute to a low likelihood that the latter two risks occur.

When compared with local, on-premise hosting, Google as a cloud provider offers better guarantees for the timely detection of risks, and for the implementation and monitoring of up-to-date security measures.

However, Google cannot protect personal against legal orders from competent authorities outside the EEA. There is therefore a non-negligible risk that local authorities outside the EEA, in particular US law enforcement authorities, may gain access to the personal data processed by Dutch government organisations. Such access is formally unlawful under the GDPR in the absence of a Mutual Legal Assistance Treaty.

As explained in Section 7 of this report, Google allows customers to store the Customer Data *at rest* from some of the Core Services in data centres in the EU. Furthermore, Google transfers personal data in Customer Data to the United States with the guarantees of the EU Standard Contractual Clauses. At the time of completion of this DPIA, personal data in Customer Data from other Core Services, Features, the Additional Services, the Google Account, Technical Support Services and Other Related Services, as well as all Diagnostic Data were transferred to the USA on the basis of the EU-US Privacy Shield agreement. Google self-certified its compliance with this privacy regime. After the Schrems-II ruling, Google only relies on Standard Contractual Clauses for the transfer of personal data from the EU to the USA.

Although both of these transfer mechanisms are legally valid and approved by the European Commission, there are doubts about the future validity of these instruments with regard to transfers to the US. Both instruments are subject to proceedings before the European Court of Justice. The Court will decide whether these agreements provide sufficient protection against the risks of mass surveillance in the United States.

These risks (of unlawful access to personal data by law enforcement, security services and intelligence agencies in the US) do not only apply to data processed in the USA, but also to the Customer Data stored in the EU. On the basis of the CLOUD Act, US law enforcement agencies may demand access to data under the control of US companies, even if those data are stored in data centres outside the territory of the United States.

Google is transparent about the amount of government requests it receives and has resisted requests it considered invalid. On 5 May 2020, Google provided separate statistics about such requests made with respect to G Suite Enterprise services customers. The report shows that between July 2019 and December 2019, Google received one request for disclosure of G Suite Enterprise service customer information from Dutch law enforcement authorities. Overall, Google received 274 requests for G Suite Enterprise data, relating to 425 customers. In 55% of requests, Google disclosed data. In the same period, Google received 486 requests for consumer data from Dutch authorities. Google's statistics are arranged per requesting country, not per nationality of the data subjects. Thus, these numbers do not provide insight how frequently data from Dutch customers of G Suite Enterprise have been requested by, or disclosed to, foreign law enforcement authorities. However, because the overall number of requests for Enterprise data is low, the risk of unlawful disclosure to foreign governments seems low.

Under the G Suite DPA, which applies only to Customer Data from the Core Services, Google is contractually bound to inform its customers if it receives such a request,

unless it is not allowed to disclose the request (a co-called 'gagging order'). The undertaking to forward of law enforcement requests to the customer do not yet apply to (i) Customer Data that may be processed through Additional Services, Technical Support Services, the Feedback form and all Diagnostic Data.

In its (consumer) Privacy Policy, Google writes: "*We'll process your data when we have a legal obligation to do so, for example, if we're responding to legal process or an enforceable governmental request.*" The words enforceable governmental request are hyperlinked to a pop-up with a reference to Google's Transparency Report and the assurance: "*Our legal team reviews each and every request, regardless of type, and we frequently push back when a request appears to be overly broad or doesn't follow the correct process.*"

The risks associated with the transfer of personal data to a provider outside the EEA are not specific to Google, but apply to all cloud service providers. All cloud service providers must necessarily collect data on the interaction of users with their servers (functional data), and may need to store some of these data as Diagnostic Data.

As assessed by the EDPB and the EDPS in their joint opinion to the LIBEL Committee of the European Parliament on the US CLOUD Act, transfers of personal data must comply with Articles 6 (principles) and 49 (exceptions allowing transfers) of the GDPR. If there is an order on the basis of the US CLOUD Act, the transfer can only be lawful if it is based on an international treaty. The supervisory authorities stress the need for new MLATs and the need to negotiate an international treaty between the EU and the US on cross-border access to electronic evidence for judicial cooperation in criminal matters.

It is up to the European Court of Justice to assess the validity of the Privacy Shield and the EC Standard Contractual Clauses for the transfer of data from the EEA to the US, and up to the European Commission to negotiate a new mutual legal assistance treaty with the US, as well as a treaty on access for law enforcement services.

It is up to the government organisations to determine what risks they consider acceptable related to the transfer of personal data to the USA. Depending on the sensitivity and confidentiality of the data, they may also decide to use only local storage for some data, or to use only local accounts.

Overall, when using G Suite Enterprise, the likelihood of the occurrence of unlawful access by US law enforcement agencies is remote, while the consequences for data subjects can vary from low to very serious. This results in a low risk for data subjects.

16.2.12 *Chilling effects employee monitoring system*

As explained in Section 2.2, government organisations have access to 19 different log files (Diagnostic Data) about the use of G Suite Enterprise by their employees. If they combine the information about individual login and email behaviour with the use of the different Core Services, the administrators could gain detailed knowledge of an individual's work patterns and lifestyle.

The log files may contain confidential or business-sensitive substantive information, such as file names and subject lines of email, and sensitive and special categories of personal data of all kinds, not only of government employees, but also of other data subjects, such as senders or recipients of, for example, email.

Government employees may feel unable to exercise their right to (moderately) make use of government facilities without being observed and to communicate about private affairs, such as sending an email to a friend or family member.

The Data Protection Authorities in the EU write in their opinion about monitoring in an employment context: *“Technologies that monitor communications can also have a chilling effect on the fundamental rights of employees to organize, set up workers’ meetings, and to communicate confidentially (including the right to seek information). Monitoring communications and behaviour will put pressure on employees to conform in order to prevent the detection of what might be perceived as anomalies, in a comparable way to the way in which the intensive use of CCTV has influenced citizens’ behaviour in public spaces. Moreover, owing to the capabilities of such technologies, employees may not be aware of what personal data are being processed and for which purposes, whilst it is also possible that they are not even aware of the existence of the monitoring technology itself.”*²⁹⁸

There is an additional risk for some types of government employees if the log files relating to for example storage of documents in Google Drive reveal that they are regularly working with Classified Information or otherwise government sensitive materials. The employees could become the targets of spear phishing (a scam via email or other electronic communication that is specifically aimed at an individual or organisation), social engineering (an attack technique that exploits human characteristics such as curiosity, trust and greed in order to obtain confidential information or have the victim carry out a certain act) or blackmail.

Therefore it is essential that access within the government organisations to the audit logs is highly restricted, that access to these logs is logged and monitored and that government organisations expand their existing internal privacy policy with detailed rules for what specific purposes personal data in the log files may be (further) processed and analysed. This includes listing the specific risks against which the logs will be checked, and what measures the organisations will take to ensure purpose limitation

Government organisations could potentially use the detailed information in the audit log files for a negative performance assessment. The likelihood of occurrence of these risks is more likely than not. This could well cause a *chilling effect*. Out of fear of being monitored, employees could start to behave differently, be inhibited from becoming a whistle-blower or for example contact certain people. This would not only infringe on their privacy rights, but also impede their exercise of related fundamental rights such as the freedom to send and receive information. Given the dependence of employees of the use of G Suite Enterprise once their organisation has chosen to work with it, they have no means to avoid this monitoring of their behaviour. The consequences for data subjects can be very serious, up to and including wrongful dismissal.

Based on the case law of the European Court of Human Rights , government organisations need to expand on their internal privacy policies, and in particular disclose to employees under which circumstances and for which specific purposes these data may be processed. It is likely that government organisations already have such rules. Therefore, the probability that these risks will occur, can be estimated as very low. Because of this remote chance, even though the impact may be very high, the data protection risks for the employees are low.

16.2.13 *Impossibility to remove individual historical Diagnostic Data*

Google generally retains Diagnostic Data from the Core Services for 180 days, but sometimes shorter, and sometimes longer. In response to questions raised during this DPIA, Google explained that the retention period for Diagnostic Data varies per use case.

²⁹⁸ Article 29 Working Party (now: EDPB), WP 249, Opinion 2/2017 on data processing at work, p. 9-10.

Google does not yet publish information about the retention periods of Diagnostic Data consisting of telemetry and website data, but has announced it will be more transparent in a future Enterprise Privacy Notice. After completion of this report, on 12 November 2020 Google published a Google Cloud Privacy Notice.²⁹⁹ This notice does not describe any specific retention periods.

Google explained it is not possible for administrators to delete individual historical Diagnostic Data. Administrators can only achieve this by deleting the Google Account on the customer domain. In case of active deletion of personal data in Customer Data, the same retention period of 180 days applies.

The GDPR requires that personal data may only be stored as long as necessary for the purposes for which they were collected. The chance that a privacy risk occurs is per definition higher with a long retention period, due to an increased risk of unlawful processing, data becoming inaccurate/outdated and data breaches.

If Google provides contractual guarantees that it will not process data for which an active deletion request is made, for any other purpose, and it will not anonymise these data for reuse in statistics, the impact of this risk for data subjects can be low. Therefore, the data protection risks for the employees are low.

16.3 Summary of risks

These circumstances and considerations as explained above lead to the following 10 high and 3 low data protection risks for data subjects:

1. Lack of purpose limitation Customer Data: loss of confidentiality, loss of control, risk of reidentification
2. Lack of purpose limitation Diagnostic Data: Loss of control , unlawful processing
3. Lack of transparency Customer Data: loss of control
4. Lack of transparency Diagnostic Data: loss of control and risk of reidentification
5. No legal ground for Google and government organisations: Loss of control, unlawful processing
6. Missing privacy controls for admins and end users: Loss of control and loss of confidentiality
7. Privacy unfriendly default settings: Loss of control and loss of confidentiality
8. One Google Account: loss of control, loss of confidentiality
9. Lack of control over subprocessors: loss of control, loss of confidentiality
10. Inability to exercise data subjects rights
11. Cloud provider: unlawful access to content and metadata: loss of control, loss of confidentiality, reidentification of pseudonymised data and unlawful (further) processing
12. Employee monitoring system: chilling effects to exercise (related) rights
13. Impossibility to remove historical Diagnostic Data: increased risk of reidentification of pseudonymised data and unlawful (further) processing

²⁹⁹ Google, Google Cloud Privacy Notice, 7 December 2020, URL: <https://cloud.google.com/terms/cloud-privacy-notice>

Based on the ICO model, this results in the following matrix:

Severity of impact	Serious harm	Low risk 11, 12, 13	High risk 8	High risk 1, 2, 3, 4, 5, 6, 7,9, 10
	Some impact	Low risk	Medium risk	High risk
	Minimal impact	Low risk	Low risk	Low risk
		Remote	Reasonable possibility	More likely than not
		Likelihood of harm (occurrence)		

Part D. Description of risk mitigating measures

Following the Dutch government’s DPIA model, Part D describes the proposed counter-measures against the data protection risks identified in part C.

The following section contains a table of the mitigating technical, organisational and legal measures that can be taken by Google and by the government organisations.

17. Risk mitigating measures

The previous Section discussed the data protection risks for data subjects. There are ten high and three low remaining risks. The government organisations can lower or mitigate some of these risks through technical and organisational measures, but most of the high risks can only be mitigated by Google.

17.1 Measures against the ten high risks

10 high risks	Measures government organisations	Measures Google
Lack of purpose limitation Customer Data	Agree on contractual purpose limitation	Become a data processor. Amend contract to provide limitative list of specific and explicit purposes for the processing of specific data
		Exclude the data processing for any marketing, profiling, research, analytics or advertising purpose
		Exclude ‘compatible’ or ‘further’ processing and the 12 possible additional purposes from the (consumer) Privacy Policy
		Exclude processing of Customer Data to anonymise for statistics, for re-use of <i>Spelling and Grammar</i> data for machine learning
		Amend contract to include exhaustive list of legitimate business purposes, when Google may act as data controller
Lack of purpose limitation Diagnostic Data	Establish policies to prevent file names and path names from containing personal data	Become a data processor. Amend contract to provide limitative list of specific and explicit purposes for the processing of specific data
		Include Chrome Enterprise in G Suite Enterprise offering, or include separate ‘data processor’ browser with G Suite Enterprise
	Agree on contractual purpose limitation	Exclude data processing for any marketing, profiling, research, analytics or advertising purpose

		Amend contract to include exhaustive list of legitimate business purposes, when Google may act as data controller
Lack of transparency Customer Data	Inform employees of the possibilities for Data Subject Access Requests, access to the audit logs and self-service tools	Provide exhaustive and comprehensible information about the processing of Customer Data from the Core Services, the Features, the Additional Services, the Google Account, the Technical Support Services and the Feedback form
	Disclose and enforce retention policy / clean up obsolete data	Provide tool to provide access to the contents of Customer Data in Diagnostic Data (including telemetry data and use of Features)
		Give a clear warning to end users about Feedback
		Provide exhaustive and comprehensible documentation about the embedded Features, including the categories of data and purposes of processing
		Provide exhaustive and comprehensible information to end users upon creation of a Google Account and make this information permanently accessible
		Provide exhaustive and comprehensible information and visually clarify the difference between the three different spellingcheckers
Lack of transparency Diagnostic Data	Consider prohibiting the use of Chrome OS and the Chrome browser	Publish centrally accessible exhaustive and comprehensible documentation about the types and content of and the purposes for processing of Diagnostic Data, including data collected from cloud servers and telemetry events (atoms)
		Create a tool for end users and admins to view the telemetry data
		Provide exhaustive and comprehensible information to end users upon creation of a Google Account, must be permanently accessible
		Include Chrome Enterprise in G Suite Enterprise offering, or include separate 'data processor' browser with G Suite Enterprise
No legal ground for Google and gov. orgs.	Do not use G Suite Enterprise until the processing can be based on one or more legal grounds	Become a data processor and process only for authorised purposes, so government organisations can successfully invoke the legal grounds of contract, public and legitimate interest
		Comply with cookie legislation, e.g. the Dutch telecommunications Act for the telemetry and website data (Diagnostic Data)
		Amend the contract to become an independent data controller with respect to <i>gagging orders</i> from law enforcement

		agencies and Google’s legitimate business purposes as controller (e.g. invoicing)
Missing privacy controls	Use controls when they become available	<p>Create central controls for admins to:</p> <ul style="list-style-type: none"> • Prevent the use of the <i>Enhanced Spellchecker</i> in the Chrome browser • Prevent re-use of content from <i>Spelling and Grammar</i> for machine learning] • Limit or switch <i>Off</i> the collection of telemetry data • Change the default setting for Ads Personalization to <i>Off</i> • Prohibit the use of Additional Services • Prohibit the use of Feedback for which Google does not want to become a data processor
Privacy unfriendly default settings	Where possible, change default settings until Google has implemented adequate privacy friendly settings	Turn Off Ads Personalization
		Turn Off access to Additional Services
		Change the default setting of the Chrome browser and in the Marketplace to prevent access by default [by third parties] to Customer Data.
		Provide exhaustive and comprehensible information what the data protection consequences are if end users or administrators opt-in to privacy unfriendly settings
One Google Account	Advise end users not to sign in with multiple Google Accounts simultaneously	Shield or protect against spill-over from enterprise to consumer environment (and vice versa)
		Provide clear warnings to end users when they leave the protected enterprise environment
	If the Chrome browser is permitted: prohibit end users from signing in with a Google Account different from the enterprise domain	Prevent any data processing via the Google Play Store beyond authorised data processor purposes
		Amend contract to provide guarantees about processing of underwater links from Core Services to Additional Services such as Translate and Maps
Lack of control subprocessors		Amend contract to include meaningful control for customer to object against subprocessors of personal data, whether included in Customer Data, data relating to the Google Account, Support Data and Diagnostic Data or otherwise processed by Google
		Become data processor for the processing of personal data in Customer Data and Diagnostic Data from the Core Services, the Features, the Additional Services, the Technical Support Services, the Google Account and the Feedback form and only engage authorised subprocessors

No access for data subjects	Inform employees about access to the data in the available admin log files	Honour data subject access rights, including with respect to all personal data in Diagnostic Data [collected through the Core Services, the Additional Services, the Features, the Google Account, the Technical Support Services and the Other Related Services. Develop tools to allow data subjects access to personal data when they are collected.
	When available, use other tools	

17.2 Measures against the three low risks

There are three low data protection risks. These stem from the lack of transparency, which could make employees think they are constantly being watched, the lack of an effective removal option for historical personal data, and the fact that Google is a cloud provider and processes personal data on servers in the United States.

Three low risks	Measures government organisations	Measures Google
Chilling effects employee monitoring system	Complement internal privacy policy for the processing of employee personal data with rules for what specific purposes specific personal data in the log files may be (further) processed and analysed. This includes listing the specific risks against which the logs will be checked, and which measures the organisations will take to ensure purpose limitation	-
Impossibility to delete individual Diagnostic Data	As soon as technically possible: minimise the collection of Diagnostic Data (including telemetry and website data)	Conduct audits on data minimisation and compliance with retention periods
		Data minimisation: create a control for individual deletion Diagnostic Data without deleting the Google Account
		Guarantee that data for which deletion is requested, will not be processed for any other purpose incl. anonymisation
Cloud provider: unlawful access to Customer Data and Diagnostic Data in the USA	Follow guidance from SLM Microsoft Rijk on ECJ Jurisprudence about transfer of personal data to the USA	Consider the creation of an EU cloud
		Data minimisation by improving the privacy controls

17.3 Conclusions July 2020

This DPIA shows that -at the time of completion of this report on 9 July 2020- there were 10 high, and 3 low data protection risks for data subjects when government organisations decide to use G Suite Enterprise. Because of the lack of transparency and purpose limitation, Google currently does not qualify as data processor for the processing of any of the personal data it collects in and about the use of G Suite Enterprise.

As explained in this DPIA, Google and the government organisations are joint controllers, but they cannot successfully claim any legal ground for the processing, as required in Article 6 of the GDPR. Until Google becomes a data processor, not only for the personal data in Customer Data, but also for the personal data in Diagnostic Data and other data described in this report such as personal data relating to the Google Account, government organisations are advised not to use G Suite Enterprise.

17.4 Google measures 12 February 2021

SLM Microsoft Rijk provided Google with the DPIA findings upon completion of this DPIA. Between August and January 2020, SLM Microsoft Rijk and Google discussed measures to mitigate the ten high data protection risks.

Google announced or already implemented several technical and organisational measures to mitigate high risks, especially with regard to Customer Data. In a privacy amendment on the framework contract, Google agrees to only process the Customer Data for three authorised purposes. In December 2020 Google published extensive information about its different services and privacy settings in the *Google Workspace Data Protection Implementation Guide*. Google has clarified that it performs all data processing of the Enterprise Account Data and use of the Features, when used in the Core Workspace Services, exclusively in a role as data processor, for the three authorised purposes. The negotiated privacy amendment prohibits Google from processing Customer Personal Data and/or Service Data for Advertising purposes or for profiling, data analytics and market research.

Google has taken extra measures to prevent spill-over of personal data from the enterprise to the consumer environment. When an employee accesses an Additional Service such as Google Search with a work account, Google ensures that the employee is automatically logged-out. Google also grants the Dutch government an effective audit right to verify compliance with the agreed processing.

Unfortunately, only two of the 10 high risks have (yet) been completely mitigated through the negotiated privacy amendment and additional improvement measures taken or announced by Google. The risks with regard to *the use of one Google account* in the work and consumer context, and with regard to *privacy unfriendly default settings*, have been or can be effectively mitigated.

Google does not expressly commit to only process Customer Personal Data when proportionate, while processing for the three authorised purposes is logical for Diagnostic Data and Support Data, but not for the processing of Customer Personal Data. Google does not want to become a data processor for the different kinds of Diagnostic Data on the individual use of the Workspace services, or for the Support Data when a customer files a Support Request (different from giving a Support employee live access to personal data), or for information provided through the Feedback form. Google does not acknowledge its role as joint controller either for these types of data processing. Google does not follow the recommended measures to include Chrome Enterprise in its Google Workplace offering, or include a separate 'data processor' Chrome browser on Android devices and Chromebooks (where installing another browser is not a realistic option). It is up to the data protection

authority to assess whether Google's arguments are convincing that it can operate as an independent data controller for the Diagnostic Data, the Support Data, the Feedback data and data collected via the use of the Chrome browser.

Though Google publishes a new list of 17 purposes for which it allows itself to process Diagnostic Data, Support Data and data from the Feedback form (called *Service Data* by Google), the description of the purposes is too vague, and not specific enough. The description does not allow government organisations or data subjects to determine what kind of processing is and is not included within these purposes. Google can unilaterally change these purposes, and only needs to give its Enterprise customers a warning in advance. If the Enterprise customers do not agree, they can only object by terminating the contract.

Google has taken two important steps to improve transparency, by publishing the Google Cloud Privacy Notice and the Google Workspace Data Protection Implementation Guide. However, these two sources fail to provide insight in (i) the exact personal data Google processes, (ii) the different retention periods and their necessity and, (iii) processors and third parties that can process personal data from Enterprise customers.

In its improvement plan Google commits to making more information available about the Diagnostic Data by the end of 2021. However, the quality of this information can only be assessed after its publication. Google declines to provide a tool for end-users or admins to inspect the telemetry data, nor will Google create a control for admins or end-users to block or minimise the amount and contents of the telemetry data sent to Google.

Google commits to create a new option for admins to export individual personal data from the audit logs. However, with regard to other categories of personal data for which Google qualifies itself as independent data controller, Google only commits to provide a better explanation when it does not give data subjects access to certain personal data, such as the Telemetry Data, Website Data and personal data from Google's SIEM security logs. It is up to the Data Protection Authority to assess whether Google's arguments are convincing that it cannot identify the user of cookie data, and in other circumstances, can rely on the exceptions in articles 12(2), 15(4) and 23 of the GDPR to not provide access.

Additionally, as a result of the jurisprudence in *Schrems-II* of the European Court of Justice, the transfer of personal Diagnostic Data to the USA needs to be reassessed. This reassessment will have to be based on the finalised guidelines of the EDPB on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.³⁰⁰

³⁰⁰ The draft version for public consultation is available at: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en.

Risk mitigating measures taken by Google³⁰¹

	High Risk	Mitigating measure Google	Remaining high risk
1	Lack of purpose Limitation Customer Data	Process Customer Personal Data as data processor only for three purposes: <ol style="list-style-type: none"> 1. <i>to provide and improve the Services and TSS subscribed to by Customer;</i> 2. <i>to identify, address and fix security threats, risks, bugs and other anomalies</i> 3. <i>to develop, deliver and install updates to the Services subscribed to by Customer (including new functionality related to the Services subscribed to by Customer).</i> 	<p>Google does not expressly commit to only process Customer Personal Data when proportionate, while the three authorised purposes are logical for Diagnostic Data and Support Data, but not for the processing of Customer Personal Data.</p> <p>Google does not want to explicitly exclude the further processing of Customer Personal Data to detect illegal activity without first obtaining prior written approval of the Customer (see p. 72 of this DPIA report). Google also does not yet provide controls to Enterprise customers to override or evade scanning, filtering or other analysis of spam and malware when such data are necessary for the employees' work duties, where commercially, technically and reasonably possible.</p> <p><u>This leads to a high risk for the many different categories of data subjects affected by the data processing.</u></p>
		Contractual exclusion of specific processing purposes: Google will not process Customer Personal Data and/or Service Data for Advertising purposes or for profiling, data analytics and market research (...)	Risk mitigated
		Assurance that machine learning to improve the contents of Spelling and Grammar Data is limited to within the customer's own Enterprise domain	Risk mitigated
		Definition of anonymisation included in the privacy amendment, in accordance with WP29 guidance	Risk mitigated for all types of personal data (also Service Data)
		The framework contract specifies how Google deals with <i>gagging orders</i> . The new list of purposes in the Google Cloud Privacy Notice	Risk mitigated for which purposes Google may lawfully process Customer Data as independent data controller.

³⁰¹ Risks that are or can be mitigated are highlighted in light-grey.

		(GCPN) only applies to Service Data, not to Customer Data	
2	Lack of purpose Limitation Diagnostic Data	<p>Google qualifies itself as (independent) data controller for the processing of <i>Service Data</i> and publishes a list of purposes in the GCPN. Service Data include all Diagnostic Data (including telemetry data), Support Data, Feedback Data and all settings/configuration chosen by Enterprise customers. Google lists 12 (combined) purposes, but 17 different purposes can be distinguished.</p> <ol style="list-style-type: none"> 1. <i>Provide Cloud Services you request including</i> 2. <i>Securing your data and services you use</i> 3. <i>Make recommendations to optimize use of Cloud Services, including information about new or related products</i> 4. <i>Maintain and</i> 5. <i>improve Cloud Services</i> 6. <i>Provide [other services] and</i> 7. <i>improve other services you request and</i> 8. <i>improve other services that you and our customers request</i> 9. <i>Assist you [read: provide TSS] and</i> 10. <i>improve online support</i> 11. <i>Protect you, our users, the public and Google against fraud, abuse, security risks and technical issues</i> 12. <i>Comply with legal obligations</i> 13. <i>Other purposes with your consent</i> 14. <i>use Service Data together with information we collect from other Google products and services</i> 15. <i>use algorithms to recognize patterns in Service Data</i> 16. <i>manually collect and review of Service Data, such as when you interact directly with our billing or support teams; and/or</i> 17. <i>aggregate and anonymize Service Data to eliminate personal details including for internal reporting and analysis of product and business operations</i> 	<p>The purposes set out in the GCPN are <u>not specific and detailed enough</u>:</p> <p>(i) Data controllers need to know when, for what purpose, Google will apply the four different processing <i>methods</i> (purpose 14 – 17) to the different categories of personal data contained in the Diagnostic Data. As the GCPN does not contain such an explanation, these four methods have to be considered as separate purposes.</p> <p>(ii) Through the GCPN, Google permits itself to use Diagnostic Data for big data analytics, to combine Diagnostic Data with personal data from other Google products, as well as a to improve other services that other customers request. These purposes are not detailed enough to determine what kind of processing is and is not included within the specified purpose, nor do they allow that compliance with the law can be assessed and data protection safeguards applied. This leads to the remaining high risk of unlawful (further) processing of personal data relating to government employees.</p> <p>(iii) The list of purposes in the GCPN seems to omit certain logical purposes, such as the use of account data for license verification and marketing sent to sales or procurement officials. This high risk can be mitigated if Google clearly distinguishes between the different purposes, explains when it applies the 4 processing methods, and adds (at least) the purposes of (1) billing (2) license verification and (3) sales communication/marketing to sales and procurement relations as three separate purposes.</p>

			<p>(iv) With respect to purpose 13 ('other purposes with your consent'), Google provided two options for a commitment in the negotiated Privacy Amendment:</p> <ol style="list-style-type: none"> 1. Google will not ask for consent where such consent is not available under the GDPR or 2. Google will not ask end users for consent to add purposes, unless required by law or with prior notice to Customer. <p>Both options do not provide sufficient safeguards. Under option 1, Google may still add purposes where it considers consent to be available. Under option 2, Google can always ask for consent provided it has given prior notice.</p>
		<p>Google does not follow the recommended measures to include Chrome Enterprise in G Suite Enterprise offering, or include separate 'data processor' Chrome browser on Android devices and Chromebooks (where installing another browser is not realistic)</p>	<p>The processing of Diagnostic Data (separate from the Google Workspace Diagnostic Data) through the Chrome browser and on Chromebooks is not subjected to the Google Cloud Privacy Notice but to Google's consumer privacy statement. Though government organisations can mitigate this risk by prohibiting the use of Android devices and the Chrome browser, this leads to loss of functionality (no possibility to work offline in Gmail or Drive when working with a browser other than Chrome), and is thus unlikely to happen. Therefore, this is a <u>remaining high risk with regard to the use of Chrome</u>.</p>
3	Lack of transparency Customer Data	<p>In the Google Workspace Data Protection Implementation Guide Google provides comprehensible information about the rules and settings for Customer Data from the Core Services, the Features, the Additional Services, the Google Account, the Technical Support Services and the Feedback form</p>	<p>Risk mitigated</p>
		<p>Google will not build a tool to provide access to the contents of Customer Data in Diagnostic Data (including telemetry data and use of Features)</p>	<p>This could lead to a <u>remaining high or low risk</u>, depending on (i) the quality of Google's documentation of the contents of telemetry and website data, and (ii) of the quality of Google's reply to Data Subject Access Requests for telemetry and cookie data (see separate risk</p>

			exercise of data subjects rights below)
		Google provides a new warning to end users in the Feedback form not to share sensitive data with Google	Risk <u>partially mitigated</u> . Government admins can further mitigate by warning employees not to use this tool.
		Explanation in the Google Data Protection Implementation Guide that the embedded Features are part of the Core Services, and only processed for the 3 authorised processor purposes	Risk mitigated
		Improved explanation to admins in the Data Protection Implementation Guide that Google processes the work account data as processor when used in the Core Services. For users, some information is permanently accessible via the Google account icon.	Risk mitigated
		<p>Google has not announced measures to provide exhaustive and comprehensible information and visually clarify the difference between the three different spellingcheckers</p> <p>Google explains in the Data Protection Implementation Guide that Chrome browser and Chrome OS are consumer products that are not part of the Google Workspace contract. Google recommends admins to buy the separate product Chrome Enterprise (out of scope of this DPIA). Google added in reply to this table that admins can also prevent the use of the Chrome Advanced Spellchecker on devices with Windows and macOS. This option was not yet tested.</p>	Because prohibiting the use of the Chrome browser is highly impractical in practice on Android devices and Chromebooks, and Google has not announced any visual improvements in the interface for the different spelling checkers used by end-users, the processing of Customer Data via the Enhanced Spellchecker in Chrome leads to a remaining high risk
4	Lack of transparency Diagnostic Data	Google has committed to publish comprehensive details about the types and content of and the purposes for the processing of Diagnostic Data, including data collected from cloud servers and telemetry events (atoms), in a help center article, the latest by 30 June 2021. The level of detail should be sufficiently high for SLM Microsoft Rijk to verify Google's compliance in an audit.	This announced measure can <u>lower this risk</u> , but needs to be assessed after publication and after the first audit organised by SLM Microsoft Rijk.
		In spite of its assurance to the researchers contained in this DPIA	With the current lack of information about the retention

		<p>that Google would publish more detailed information about the retention periods of the Diagnostic Data in a future Privacy Notice, in the GCPN Google only writes: <i>"We retain Service Data for different periods of time depending on what it is, how we use it, and how you configure your settings. Service Data is deleted or anonymized once it is no longer needed."</i></p> <p>Google also explains: <i>"For each type of data and operation, we set retention timeframes based on the purpose for its collection."</i> Google indicated that it expects to update the GCPN in the next 12 months but did not specify of the contents of the update.</p>	<p>periods, even though Google has determined retention timeframes per purpose, Google violates the transparency requirements of Articles 13(2)a and 14(2)a of the GDPR. Google has not provided a commitment that it will update the GCPN to address this specific issue. This leads to a <u>high risk</u></p>
		<p>Google does not publish a limitative list of processors it may share Service Data with. In the GCPN Google writes: <i>"We provide information to our affiliates, partners and other trusted businesses or persons to process it for us, based on our instructions and in compliance with this Privacy Notice and other appropriate confidentiality and security measures."</i> Google expects to update the GCPN in the next 12 months (without specification of the contents of the update).</p>	<p>See the <u>high risk addressed below</u> of lack of control over the sharing by Google of Service Data with third parties With its current lack of specific information Google violates Article 13(1)e and 14(1)e of the GDPR. Google has not provided a commitment that it will update the GCPN to address this specific issue.</p>
		<p>Google will not create a tool for end users and admins to view the telemetry data</p>	<p>Possible remaining risk related to the quality of Google's reply to Data Subject Access Requests with regard to telemetry and cookie data (see separate risk relating to the exercise of data subjects rights)</p>
		<p>Information about the privacy conditions of the use of a Google Work account will be made permanently accessible through the account icon. End-users are no longer requested to tick a consent box to create the account.</p>	<p>Gov admins can help lower this risk prior to July 2022 by providing high-over information to employees based on the information in the Data Protection Implementation Guide.</p>
5	No legal ground for Google and gov. orgs.	<p>Although Google has stated that it is willing to assess the feasibility to changing its role for Service Data in the future, currently Google does not want to become a data processor for the Diagnostic Data, Support Data and Feedback Data, and does not acknowledge a role</p>	<p>Though Google assumes it is possible to separate its role as processor for the Customer Data from its role as data controller for the Service Data, this report concludes that is not possible, because of the inextricable link between the two categories of</p>

		as joint controller with the government organisations either.	data. Google and the Dutch government have to be qualified as joint controllers for the processing of the Diagnostic Data, but Google and the Dutch government do not have a joint controller agreement as foreseen in Article 26 GDPR. If government organisations disclose personal data to Google as a third party, they cannot successfully invoke the legal grounds of contract, public and legitimate interest. There is no commitment from Google to switch to a processor role. <u>This leads to a high risk.</u>
		With regard to the legal ground for the collection of cookie and telemetry data from end-user devices Google states it employs cookies and similar technologies that are necessary to enable the services to function. Google also explains it works <i>to improve our transparency and compliance as necessary in response to the evolving regulatory landscape relating to e-Privacy.</i>	Google will publish more information about the contents and purposes of the telemetry and website data the latest by end of 2021. Given the current lack of transparency about the contents and purposes of the telemetry and website data, Google cannot rely on the two legal exceptions on the consent requirement. This currently also leads to a <u>high risk</u> , also because nor admins nor end-users can minimise the telemetry data processing
		Amend the contract to become an independent data controller with respect to <i>gagging orders</i> from law enforcement agencies and Google's legitimate business purposes as controller (e.g. invoicing)	Risk mitigated
6	Missing privacy controls	<p>Google provides assurances about, or enables admins to take, 4 of the 6 recommended measures:</p> <ul style="list-style-type: none"> • Google will not re-use of content from <i>Spelling and Grammar</i> for machine learning outside of the Enterprise customer's domain • Admins can prohibit the use of Additional Services through consumer accounts when logged in with a work account • Admins can prevent the use of the Enhanced Spellchecker in the Chrome browser on macOS and Windows by applying settings in the MacOS preferences file, or by applying group policies, but this 	<p>There are two remaining risks with regard to telemetry data and with regard to Feedback data.</p> <p>Google does not offer a choice to limit or switch <i>Off</i> the collection of telemetry data. This leads to a <u>high risk</u> in view of the following 4 circumstances:</p> <ol style="list-style-type: none"> 1. Google currently makes no information available about the contents of these data 2. Google permits itself to process these data for the 17 broad purposes defined in the GCPN 3. Google will not create a telemetry viewer tool, and

		<p>solution does not work for Chromebooks, Android and iOS mobile devices. Admins can only prevent this processing on these devices by procuring the separate Chrome Enterprise product (out of scope of this DPIA).</p> <ul style="list-style-type: none"> Google will change the default setting for new users for Ads Personalization to Off 	<p>4. Personal data were observed in the technical tests conducted for this DPIA, including sensitive data.</p> <p>As discussed above, <u>admins can lower the risk</u> of a missing central Feedback control by warning employees not to use this module.</p>
7	Privacy unfriendly default settings	<p>Google has announced to partially implement 4 of the 5 recommended measures to change its default settings:</p> <ol style="list-style-type: none"> Admins can disable access to the existing Additional Services (but not to any new services). Google will change the default setting for new users for Ads Personalization to Off Google provides new explanations about the privacy settings in the Workspace Data Protection Implementation Guide Google will not ask for consent from employees for Service Data 	<p>Admins can (and should) lower the remaining 3 risks:</p> <ol style="list-style-type: none"> Turn off access to new Additional Services when they appear Change the default setting of the Chrome browser (if used at all) and in the Marketplace to prevent access by default [by third parties] to Customer Data, and Instruct existing users to turn Off Ads Personalisation
8	One Google Account	<p>Google will implement the 4 recommended measures:</p> <ol style="list-style-type: none"> Google enables admins to block the use of consumer Google accounts in the Workspace environment. This prevents the risk of spill-over of personal data from the enterprise to consumer environment (and vice versa). Google will provide a prominent visual indicator in the form of the user profile picture on the landing page for all Workspace Core Services to make it clear to the user that they are in the enterprise environment. The user profile picture will be absent when the end user is not in the enterprise environment. Google has provided a contractual guarantee that traffic from Core Services to Additional Services such as Translate, and Maps is 	<p>Risks mitigated or will be mitigated</p>

		<p>processed within the processor-domain.</p> <p>Google currently offers free access to admins to the Play Store for Work, for end-users to download the Device Policy App</p>	
8	One Google Account	<p>Google will implement the 4 recommended measures:</p> <p>5. Google enables admins to block the use of consumer Google accounts in the Workspace environment. This prevents the risk of spill-over of personal data from the enterprise to consumer environment (and vice-versa).</p> <p>6. Google will provide a prominent visual indicator in the form of the user profile picture</p> <p>7. on the landing page for all Workspace Core Services to make it clear to the user that they are in the enterprise environment. The user profile picture will be absent when the end-user is not in the enterprise environment.</p> <p>8. Google has provided a contractual guarantee that traffic from Core Services to Additional Services such as Translate, and Maps is processed within the processor-domain.</p> <p>Google currently offers free access to admins to the Play Store for Work, for end-users to download the Device Policy App</p>	Risks mitigated or will be mitigated
9	Lack of control third parties / (sub-) processors	<p>Google only uses subprocessors for Customer Personal Data in the support requests.</p> <p>However, as self-qualified controller for the Service Data, Google gives its Enterprise customers no information or control over the third parties with which it may share personal data.</p>	<p>In view of the limited set of personal Customer data that Google wants to share with subprocessors, and the contractual guarantees that Google will comply with the GDPR, also when using subprocessors, the lack of control over new subprocessors for Customer Data can be reassessed as a <u>low risk</u>.</p> <p>The lack of control over Google's unknown processors or third parties for the Diagnostic Data, Support Data and data in the Feedback form, parties that may each engage other unknown</p>

			third parties / subprocessors, remains a <u>high risk</u> .
10	No access for data subjects	With regard to the Diagnostic Data Google already makes available for admins, Google commits to create a new individual take-out possibility. Google also commits to provide a better explanation to end-users, by July 2021, when it doesn't provide access to personal data. For example, Google does not include data if providing a copy of such data would adversely affect the rights and freedoms of others. Also, by design, Google does not provide exact copies of any raw log data, as that might enable a malicious actor to construct attack scenarios that could lead to significant harm.	There is a <u>remaining high risk</u> that Google will not provide the required access to the personal data contained in telemetry and cookie data, as demonstrated in section 2.4 of this DPIA, and assessed in section 15.3. After July 2021, it needs to be assessed whether Google's arguments are convincing that it cannot identify the user of cookie data, and in other circumstances, can rely on the exceptions in article 23 of the GDPR to not provide access.

CONCLUSIONS

In sum, the use of Google Workspace as offered under the privacy amendment of the Dutch government, still leads to 8 high risks for the different categories of data subjects involved (not just employees, but all kinds of other data subjects that may interact with the Dutch government).

SLM Microsoft Rijk proceeds by engaging in a prior consultation procedure with the Dutch Data Protection Authority.