



# Independent Audit on Google Search - Digital Services Act

For the Period of 1 June 2024 to 31 May 2025

With Assurance Report of Independent Accountants regarding Regulation (EU) 2022/2065, the Digital Services Act (DSA)

# Table of Contents

Report of Management of Google Ireland Limited on Google Search’s Compliance with the Digital Services Act .....1

Attachment A - Listing of DSA sub articles, designating management’s determinations .....2

Assurance Report of Independent Accountants – Digital Services Act .....6

Appendix 1 — Description of additional information on each of the applicable audit obligations (documentation and results of any tests performed by the auditing organization, including as regards algorithmic systems of the audited provider), including summaries of conclusions reached .....10

Appendix 2 – Overview of methodology/approach of procedures performed .....85

Appendix 3 — Annex I of the Delegated Regulation — Template for the audit report referred to in Article 6 of Delegated Regulation .....88

Appendix 4 — Written agreement(s) between audited provider and the auditing organization.....95

Appendix 5 — Documents relating to the audit risk analysis .....96

Appendix 6 — Documents attesting that the auditing organization complies with the obligations laid down in Article 37(3), point (a), (b), and (c) ..... 101

Appendix 7 — Definitions ..... 102



**Google Ireland Limited**

Registered office address: Gordon House, Barrow Street, Dublin 4, D04 E5W5, Ireland

## **Report of Management of Google Ireland Limited on Google Search's Compliance with the Digital Services Act**

27 August 2025

We, as members of management of Google Ireland Limited ("GIL" or the "Company") are responsible for the processes and controls implemented for Google Search (the "audited service"), designated as a Very Large Online Search Engine ("VLOSE") by the European Commission, pursuant to Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 (the "Digital Services Act" or "DSA" or "Act"), to comply with all obligations in the aggregate, as well as with each applicable individual obligation, referred to in Article 37(1)(a) of the Digital Services Act (together the "DSA Specified Requirements") during the period from 1 June 2024 through 31 May 2025 (the "DSA Examination Period"). Unless referenced otherwise, each applicable obligation is defined at the sub article level. We also are responsible for establishing and maintaining effective internal control over compliance with the DSA Specified Requirements.

In order to fulfil our responsibilities, the Company has requested that Google LLC and/or its relevant subsidiaries (including in relation to their systems, processes, and infrastructure) (i) take certain action necessary to ensure compliance with the DSA; and (ii) take action to provide access, assistance, and support, including management representations as requested by the Company, in order for the Company to comply with its professional obligations.

We have performed an evaluation of the Company's compliance with the DSA Specified Requirements, including those described below, during the DSA Examination Period.

Based on our evaluation, we assert that, except for the effects of the matter giving rise to the modification as described in Attachment A, Google Search complied with the applicable DSA Specified Requirements in the aggregate, as well as with each applicable individual DSA Specified Requirements during the DSA Examination Period, as set out in Chapter III of the DSA, in all material respects (the "DSA Assertion").

We, as members of management of the Company, are responsible for preparing this report, including the completeness, accuracy and method of presentation of this report. As such, we are responsible for:

- Determining the applicability of each obligation of the DSA during the DSA Examination Period (see Attachment A)
- Complying with the DSA Specified Requirements by designing, implementing, and maintaining the audited service's system and manual processes (and related controls) to comply with the DSA
- Selecting the DSA Specified Requirements, making legal interpretations and developing operational benchmarks, as needed, to implement the DSA Specified Requirements
- Evaluating and monitoring the audited service's compliance with the DSA Specified Requirements
- Our DSA Assertion of compliance with the DSA Specified Requirements
- Having a reasonable basis for our DSA Assertion
- Preparing our audit implementation report referred to in Article 37(6) of the DSA, including the completeness, accuracy, and method of presentation.

Furthermore, our responsibility includes maintaining adequate records and making estimates that are relevant to the preparation of our DSA Assertion and our evaluation of the audited service's system and manual processes (and related controls) in place to achieve compliance.

Management of GIL

## Attachment A - Listing of DSA sub articles, designating management's determinations

### Listing of management's determination of compliance

Section 1	Section 2	Section 3	Section 4	Section 5
11.1		24.2		34.1
11.2		24.3		34.2
11.3				34.3
12.1				35.1
12.2				36.1
14.1				37.1
14.2				37.2
14.4				37.3
14.5				37.4
14.6				37.5
15.1				37.6
				38
				39.1
				39.2
				39.3
				40.1
				40.12
				41.1
				41.2
				41.3
				41.4
				41.5
				41.6
				41.7
				42.1
				42.3
				42.4
				42.5

#### Audited Service Legend

	In compliance (positive or positive with comments)
	Partial compliance – remediated either (1) in accordance with Audit Implementation report or (2) during the DSA Examination Period (negative – except for)
	Partial compliance (negative – except for)
	Not in compliance

**Not applicable sub article summary**

Section 1	Section 2	Section 3	Section 4	Section 5
13.1	16.1	19.1	29.1	33.1–33.6
13.2	16.2	19.2	29.2	35.2
13.3	16.3	20.1	30.1-30.7	35.3
13.4	16.4-16.6	20.2	31.1-31.3	36.2-36.11
13.5	17.1	20.3-20.6	32.1	37.7
14.3	17.2	21.1	32.2	40.2
15.2	17.3	21.2		40.3-40.7
15.3	17.4	21.3		40.8–40.11
	17.5	21.4		40.13
	18.1	21.5		42.2
	18.2	21.6-21.9		43.1-43.7
		22.1		44.1
		22.2-22.5		44.2
		22.6		45.1-45.4
		22.7		46.1-46.4
		22.8		47.1-47.3
		23.1-23.4		48.1-48.5
		24.1		
		24.4		
		24.5		
		24.6		
		25.1		
		25.2		
		25.3		
		26.1-26.3		
		27.1-27.3		
		28.1		
		28.2		
		28.3		
		28.4		

**Audited Service Legend**

	Not an auditable obligation
	Not applicable until the Commission takes action
	Condition does not exist for the sub article to be applicable

## Rationale for designations of “Not applicable - Condition does not exist for the sub article to be applicable”

Sub Article	Rationale
13.1, 13.2, 13.4	These sub articles are only applicable if the providers of intermediary services do not have an establishment in the European Union (EU) but offer services in the EU. Given GIL is established in the EU, these sub articles are not applicable.
14.3	This sub article is only applicable if an intermediary service is primarily directed at minors or is predominantly used by them. Google Search is not primarily directed at minors or predominantly used by them.
16.1, 16.2, 16.4 – 16.6	These sub articles are only applicable to providers of hosting services including online platforms. These sub articles do not apply to Google Search as it is an online search engine.
17.1, 17.3	These sub articles are only applicable to providers of hosting services including online platforms. These sub articles do not apply to Google Search as it is an online search engine.
18.1, 18.2	These sub articles are only applicable to providers of hosting services including online platforms. These sub articles do not apply to Google Search as it is an online search engine.
20.1, 20.3 – 20.6	These sub articles are only applicable to providers of online platforms. These sub articles do not apply to Google Search as it is an online search engine.
21.1, 21.2, 21.5	These sub articles are only applicable to providers of online platforms. These sub articles do not apply to Google Search as it is an online search engine.
22.1, 22.6	These sub articles are only applicable to providers of online platforms. These sub articles do not apply to Google Search as it is an online search engine.
23.1 – 23.4	These sub articles are only applicable to providers of online platforms. These sub articles do not apply to Google Search as it is an online search engine.
24.1, 24.5	These sub articles are only applicable to providers of online platforms. These sub articles do not apply to Google Search as it is an online search engine.
25.1	This sub article is only applicable to providers of online platforms. This sub article does not apply to Google Search as it is an online search engine.
26.1 – 26.3	These sub articles are only applicable to providers of online platforms. These sub articles do not apply to Google Search as it is an online search engine.
27.1 – 27.3	These sub articles are only applicable to providers of online platforms. These sub articles do not apply to Google Search as it is an online search engine.
28.1, 28.2	These sub articles are only applicable to providers of online platforms. These sub articles do not apply to Google Search as it is an online search engine.
30.1 – 30.7	These sub articles are only applicable to providers of online platforms allowing consumers to conclude distance contracts with traders. These sub articles do not apply to Google Search as it is an online search engine.
31.1 – 31.3	These sub articles are only applicable to providers of online platforms allowing consumers to conclude distance contracts with traders. These sub articles do not apply to Google Search as it is an online search engine.

Sub Article	Rationale
32.1, 32.2	These sub articles are only applicable to providers of online platforms allowing consumers to conclude distance contracts with traders. These sub articles do not apply to Google Search as it is an online search engine.
40.3 – 40.7	<p>Note: The Commission has not yet adopted the delegated act on data access. Until such time, Articles 40.3 to 40.7 are not applicable.</p> <p>These sub articles are only applicable if a reasoned request from the Digital Services Coordinator (DSC) of establishment or the Commission has taken place under sub article 40.1 or 40.4. As the provider has not received any request from the DSC or the Commission during the DSA Examination Period, these sub articles are not applicable.</p>
42.2	This sub article is only applicable to providers of very large online platforms. This sub article does not apply to Google Search as it is an online search engine.



Ernst & Young LLP  
303 Almaden Boulevard  
San Jose, CA 95110

Tel: +1 408 947 5500  
Fax: +1 408 947 5717  
ey.com

## Assurance Report of Independent Accountants – Digital Services Act

To the Board of Directors of Google Ireland Limited

### Scope

We were engaged by Google Ireland Limited (“GIL”) (the “Company” or “audited provider”) to perform an assurance engagement to examine management’s assertion (the “DSA Assertion”), included in the attached *Report of Management of Google Ireland Limited on Google Search’s Compliance with the Digital Services Act*, regarding compliance of Google Search, including the processes and controls implemented for Google Search (the “audited service”), with all obligations in the aggregate, as well as with each applicable individual obligation, referred to in Article 37(1)(a) of the Regulation (EU) 2022/2065 of the European Parliament and of the Council (the “Digital Services Act” or “DSA”) (together the “DSA Specified Requirements”) for the period from 1 June 2024 through 31 May 2025 (the “DSA Examination Period”), and opine on the audited service’s compliance with the DSA Specified Requirements. Unless referenced otherwise, each applicable obligation is defined at the sub article level.

We did not perform assurance procedures on the audited service’s compliance with codes of conduct and crisis protocols (referred to in Article 37(1)(b) of the DSA and Annex I of the Commission Delegated Regulation (EU) 2024/436 supplementing Regulation (EU) 2022/2065 (the “Delegated Regulation”)) because the requirement for the audited service to comply with such articles did not exist during the DSA Examination Period.

Additionally, the information included in the audited provider’s separately provided audit implementation report, is presented by the audited provider to provide additional information. Such information has not been subjected to the procedures applied in our examination, and accordingly, we do not express an opinion, conclusion, nor any form of assurance on it.

### GIL’s responsibilities

The management of the audited provider is responsible for:

- Determining the applicability of each of the DSA’s obligations during the DSA Examination Period
- Complying with the DSA Specified Requirements by designing, implementing, and maintaining the audited service’s system and manual processes (and related controls) to comply with the DSA
- Selecting the DSA Specified Requirements making legal interpretations and developing operational benchmarks, as needed, to implement the DSA Specified Requirements
- Evaluating and monitoring the audited service’s compliance with the DSA Specified Requirements
- Its DSA Assertion of compliance with the DSA Specified Requirements
- Having a reasonable basis for its DSA Assertion
- Preparing its audit implementation report referred to in Article 37(6) of the DSA, including the completeness, accuracy, and method of presentation.

This responsibility includes establishing and maintaining internal controls, maintaining adequate records and making estimates that are relevant to the preparation of its DSA Assertion and evaluation of its audited service’s system and manual processes (and related controls) in place, such that it is free from material misstatement, whether due to fraud or error.





## Our responsibilities and procedures performed

Our responsibility is to:

- Plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the audited service complies with each of the DSA Specified Requirements
- Form an independent opinion on whether the audited service is in compliance with the DSA Specified Requirements, based on the procedures we have performed and the evidence we have obtained and
- Express our modified opinion to the audited provider.

For additional responsibilities of the Company and Ernst & Young LLP, see Appendix 4 for the engagement statement of work executed on 10 January 2025.

We conducted our examination in accordance with the *International Standard for Assurance Engagements Other Than Audits or Reviews of Historical Financial Information* ("ISAE 3000 (Revised)"), the attestation standards established by the American Institute of Certified Public Accountants ("AICPA"), applicable aspects of the Delegated Regulation and the terms of reference for this examination as agreed with GIL on 10 January 2025. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether GIL complied, in all material respects, with the DSA Specified Requirements referenced above. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material noncompliance, whether due to fraud or error. We believe that the evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our modified opinion.

Our examination included the following procedures, among others:

- Obtaining an understanding of the characteristics of the services provided by the audited provider
- Evaluating the appropriateness of the DSA Specified Requirements applied and their consistent application, including evaluating the reasonableness of estimates made by the audited provider
- Obtaining an understanding of the systems and processes implemented to comply with the DSA, including obtaining an understanding of the internal control environment relevant to our examination and testing the internal control environment to the extent needed to obtain evidence of the Company's compliance with the DSA Specified Requirements, but not for the purpose of expressing an opinion on the effectiveness of the audited provider's internal control
- Identifying and assessing the risks whether the compliance with the DSA Specified Requirements is incomplete or inaccurate, whether due to fraud or error, and designing and performing further assurance procedures responsive to those risks, and
- Obtaining assurance evidence that is sufficient and appropriate to provide a basis for our modified opinion.

We collected evidence throughout the period from 10 January 2025 through 27 August 2025 to assess the audited service's compliance with the DSA Specified Requirements during the DSA Examination Period.

## Our independence and quality management

We are required to be independent of GIL and, in accordance with Article 37(3), if applicable, any legal person connected to GIL, and to meet our other ethical responsibilities, as applicable for examination engagements set forth in the Preface: Applicable to All Members and Part 1 – Members in Public Practice of the Code of Professional Conduct established by the AICPA and other relevant ethical requirements required for our engagement.

We also apply the AICPA's quality management standards and the International Standard on Quality Management 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements*, which requires that we design, implement and operate a system of quality management including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.



Furthermore, our attestation that the auditing organization complies with the obligations laid down in Article 37(3), point (a), (b), and (c) is included in Appendix 6.

### **Description of additional information on each of the applicable audit obligations**

The audit conclusion; audit criteria, materiality thresholds, audit procedures, justification of any changes to the audit procedures during the audit, methodologies and results, including any test and substantive analytical procedures; justification of the choice of those procedures and methodologies, overview and description of information relied upon as audit evidence; explanation of how the reasonable level of assurance was achieved; notable changes to the systems and functionalities audited; identification of any specific element which could not be audited (if applicable) or audit conclusion not reached; and other relevant observations and findings associated with our audit of the obligations is included in Appendix 1 and Appendix 2. Additionally, our summary of audit risk analysis pursuant to Article 9 of the Delegated Regulation, including assessment of inherent, control, and detection risk for each of the audit obligations is included in Appendix 5. See the summary in Appendix 1 for the audit obligations not subjected to audit since they were not applicable during the DSA Examination Period.

### **Inherent limitations**

The services in the digital sector and the types of practices relating to these services can change quickly and to a significant extent. Therefore, projections of any evaluation to future periods are subject to the risk that the entity's compliance with the DSA Specified Requirements may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

The audited service is subject to measurement uncertainties resulting from limitations inherent in the nature of the audited service and the methods used in determining such systems and processes implemented to comply with the DSA Specified Requirements. The selection of different but acceptable measurement techniques, including benchmarks, can result in materially different measurements. The precision of different measurement techniques may also vary.

Our examination was limited to certain aspects of the audited service's algorithmic systems, to the extent needed to obtain evidence of the audited service's compliance with the relevant DSA Specified Requirements as required by Regulation (EU) 2022/2065. This did not include all of the algorithmic systems that Google Search operates, nor all aspects of the algorithmic systems for which we performed audit procedures. Furthermore, algorithms may not consistently operate in accordance with their intended purpose or at an appropriate level of precision. Because of their nature and inherent limitations, algorithms may introduce biases of the human programmer resulting in repeated errors or a favoring of certain results or outputs by the model. Accordingly, we do not express an opinion, conclusion, nor any form of assurance on the design, operation, and monitoring of the algorithmic systems. The performance of risk assessments, including the identification of systemic risks, is inherently judgmental. Risk assessments are often conducted at a specific point in time and may not capture the dynamic nature of risks. Because the identification of systemic risks relies on known risks and expert judgment, the identification of systemic risks may not account for new or unprecedented events for which there is limited or no historical information.

### **Emphasis of certain matters**

Applying the DSA Specified Requirements requires the audited service to develop benchmarks and make interpretations of obligations, including certain terminology. Benchmarks and interpretations for which we deemed would be needed for report users to make decisions are described in Appendix 1 for applicable obligations.

We are also not responsible for the audited provider's interpretations of, or compliance with, laws, statutes, and regulations (outside of the DSA Specified Requirements) applicable to the audited provider in the jurisdictions within which the audited provider operates. Accordingly, we do not express an opinion or other form of assurance on the audited provider's compliance or legal determinations.

Our examination was limited to understanding and assessing certain internal controls. Because of their nature and inherent limitations, controls may not prevent, or detect and correct, all errors or fraud that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods is subject to the risk that internal controls



may become inadequate because of changes in conditions, that the degree of compliance with such internal controls may deteriorate, or that changes made to the system or internal controls, or the failure to make needed changes to the system or internal controls, may alter the validity of such evaluations.

### **Audit Opinion**

The audit opinion for compliance with the audited obligations, in the aggregate, and for each individual obligation referred to in Article 37(4), point (g) of the DSA is to be phrased as Positive, Positive with comments, or Negative. Furthermore, Annex 1 of the Delegated Regulation requires an explanation for individual DSA Specified Requirements where an opinion was not able to be reached. On the basis of the conclusions for each obligation, the auditing organization is also required to include an overall audit opinion.

### **Basis for Qualified (Negative) Opinion**

As noted in Appendix 1, our examination disclosed conditions that, in the aggregate, resulted in material noncompliance of certain DSA Specified Requirements applicable to Google Search during the DSA Examination Period.

### **Qualified (Negative) Opinion**

In our opinion, except for the effects of the matter giving rise to the modification as described in Appendix 1, Google Search complied with the applicable DSA Specified Requirements during the DSA Examination Period as set out in Chapter III of the DSA, in all material respects.

### **Conclusions on each applicable individual obligation**

For conclusions on each obligation, see Appendix 1.

### **Restricted Use and Purpose**

This report is intended solely for the information and use of GIL, the European Commission and the applicable Digital Services Coordinator of establishment as mandated under DSA Article 42(4), (collectively, the “Specified Parties”) for assessing the audited provider’s compliance with the DSA Specified Requirements, and is not intended to be, and should not be, used by anyone other than these Specified Parties, including users of the service, who are not identified as Specified Parties but who may have access to this report as required by law or regulation or for other purposes.

A handwritten signature in black ink that reads 'Ernst &amp; Young LLP'.

27 August 2025



## **Appendix 1 — Description of additional information on each of the applicable audit obligations (documentation and results of any tests performed by the auditing organization, including as regards algorithmic systems of the audited provider), including summaries of conclusions reached**

Refer to **Appendix 2** for an overview of the methodology and approach of procedures performed; our evaluation and use of the audited provider’s legal interpretation, operational benchmarks and definitions (i.e., “audited provider’s developed supplemental criteria”); the impact of notable changes to the systems and functionalities audited during the DSA Examination Period; and our use of sampling.



## Audit conclusions of applicable sub articles

Section 1	Section 2	Section 3	Section 4	Section 5
11.1		24.2		34.1
11.2		24.3		34.2
11.3				34.3
12.1				35.1
12.2				36.1
14.1				37.1
14.2				37.2
14.4				37.3
14.5				37.4
14.6				37.5
15.1				37.6
				38
				39.1
				39.2
				39.3
				40.1
				40.12
				41.1
				41.2
				41.3
				41.4
				41.5
				41.6
				41.7
				42.1
				42.3
				42.4
				42.5

Color Legend	
Positive	"Unqualified"
Positive with comments	"Unqualified"
Negative	Partial noncompliance ("except for") – remediated either (1) in accordance with Audit Implementation report or (2) during the DSA Examination Period
Negative	Partial noncompliance ("except for")
Negative	Noncompliance ("adverse")



### Not applicable sub article summary

Section 1	Section 2	Section 3	Section 4	Section 5
13.1	16.1	19.1	29.1	33.1–33.6
13.2	16.2	19.2	29.2	35.2
13.3	16.3	20.1	30.1-30.7	35.3
13.4	16.4-16.6	20.2	31.1-31.3	36.2-36.11
13.5	17.1	20.3-20.6	32.1	37.7
14.3	17.2	21.1	32.2	40.2
15.2	17.3	21.2		40.3-40.7
15.3	17.4	21.3		40.8–40.11
	17.5	21.4		40.13
	18.1	21.5		42.2
	18.2	21.6-21.9		43.1-43.7
		22.1		44.1
		22.2-22.5		44.2
		22.6		45.1-45.4
		22.7		46.1-46.4
		22.8		47.1-47.3
		23.1-23.4		48.1-48.5
		24.1		
		24.4		
		24.5		
		24.6		
		25.1		
		25.2		
		25.3		
		26.1-26.3		
		27.1-27.3		
		28.1		
		28.2		
		28.3		
		28.4		

Color Legend	
	Not an auditable obligation
	Not applicable until the Commission takes action
	Condition does not exist for the sub article to be applicable



## Rationale for designations of “Not applicable - Condition does not exist for the sub article to be applicable”

Sub Article	Rationale
13.1, 13.2, 13.4	These sub articles are only applicable if the providers of intermediary services do not have an establishment in the European Union (EU) but offer services in the EU. Given GIL is established in the EU, these sub articles are not applicable.
14.3	This sub article is only applicable if an intermediary service is primarily directed at minors or is predominantly used by them. Google Search is not primarily directed at minors or predominantly used by them.
16.1, 16.2, 16.4 – 16.6	These sub articles are only applicable to providers of hosting services including online platforms. These sub articles do not apply to Google Search as it is an online search engine.
17.1, 17.3	These sub articles are only applicable to providers of hosting services including online platforms. These sub articles do not apply to Google Search as it is an online search engine.
18.1, 18.2	These sub articles are only applicable to providers of hosting services including online platforms. These sub articles do not apply to Google Search as it is an online search engine.
20.1, 20.3 – 20.6	These sub articles are only applicable to providers of online platforms. These sub articles do not apply to Google Search as it is an online search engine.
21.1, 21.2, 21.5	These sub articles are only applicable to providers of online platforms. These sub articles do not apply to Google Search as it is an online search engine.
22.1, 22.6	These sub articles are only applicable to providers of online platforms. These sub articles do not apply to Google Search as it is an online search engine.
23.1 – 23.4	These sub articles are only applicable to providers of online platforms. These sub articles do not apply to Google Search as it is an online search engine.
24.1, 24.5	These sub articles are only applicable to providers of online platforms. These sub articles do not apply to Google Search as it is an online search engine.
25.1	This sub article is only applicable to providers of online platforms. This sub article does not apply to Google Search as it is an online search engine.
26.1 – 26.3	These sub articles are only applicable to providers of online platforms. These sub articles do not apply to Google Search as it is an online search engine.
27.1 – 27.3	These sub articles are only applicable to providers of online platforms. These sub articles do not apply to Google Search as it is an online search engine.
28.1, 28.2	These sub articles are only applicable to providers of online platforms. These sub articles do not apply to Google Search as it is an online search engine.



Sub Article	Rationale
30.1 – 30.7	These sub articles are only applicable to providers of online platforms allowing consumers to conclude distance contracts with traders. These sub articles do not apply to Google Search as it is an online search engine.
31.1 – 31.3	These sub articles are only applicable to providers of online platforms allowing consumers to conclude distance contracts with traders. These sub articles do not apply to Google Search as it is an online search engine.
32.1, 32.2	These sub articles are only applicable to providers of online platforms allowing consumers to conclude distance contracts with traders. These sub articles do not apply to Google Search as it is an online search engine.
40.3 – 40.7	<p>Note: The Commission has not yet adopted the delegated act on data access. Until such time, Articles 40.3 to 40.7 are not applicable.</p> <p>These sub articles are only applicable if a reasoned request from the Digital Services Coordinator (DSC) of establishment or the Commission has taken place under sub article 40.1 or 40.4. As the provider has not received any request from the DSC or the Commission during the DSA Examination Period, these sub articles are not applicable.</p>
42.2	This sub article is only applicable to providers of very large online platforms. This sub article does not apply to Google Search as it is an online search engine.





## Section 1 — Provisions applicable to all providers of intermediary services

Obligation:	Audit criteria:	Materiality threshold:
11.1	<p>Throughout the period, in all material aspects:</p> <p>A single point of contact was designated to enable the audited service to communicate directly, by electronic means, with Member States' authorities, the Commission and the European Board for Digital Services.</p> <p><b>The following are certain operational benchmark(s) defined by the audited service:</b></p> <p>"single point of contact": one mechanism to contact the audited service for help.</p>	<p>If a control was not suitably designed and operated effectively to satisfy the obligation for at least 95% of the DSA Examination Period, and/or if there was an actual or projected error of more than 5% (or other material qualitative variance) during the DSA Examination Period related to the audit criteria.</p>
<p><b>Audit procedures and information relied upon:</b></p> <p>In order to evaluate the audited service's compliance with this DSA Specified Requirement, we performed substantive procedures, although controls existed, as outlined below:</p> <ol style="list-style-type: none"> <li>1. Conducted a walkthrough and inquired with management to gain an understanding of the single point of contact and inspected the public facing website whereat Member States' authorities, the Commission and the European Board for Digital Services can contact the audited service pursuant to Article 11. It was noted that a single point of contact has been designated for Member States' authorities, the Commission and the European Board for Digital Services for purposes of the DSA.</li> <li>2. Inspected the public facing website whereat Member States' authorities, the Commission and the European Board for Digital Services can contact the service provider pursuant to Article 11, thus confirming that there is a means for the Member States' authorities, the Commission and the European Board for Digital Services to contact the single point of contact directly and electronically.</li> <li>3. Inspected the single point of contact webpage throughout the DSA Examination Period and confirmed its existence.</li> <li>4. Inquired with management and management noted that no significant changes were made to the policies, processes and/or controls after the walkthrough had been conducted through the end of the DSA Examination Period.</li> </ol> <p><b>Changes to the audit procedures during the audit:</b></p> <p>None.</p> <p><b>Results of procedures performed, how reasonable level of assurance was achieved, and conclusion:</b></p> <p>There were no material deviations identified in the performance of the above procedures, unless denoted below. The results of the audit procedures were deemed sufficient to obtain reasonable assurance.</p>		



**Positive** – In our opinion, the audited service complied with this DSA Specified Requirement during the DSA Examination Period, in all material respects.

**Recommendations on specific measures:**

Not applicable.

**Recommended timeframe to implement specific measures:**

Not applicable.

**Obligation:**

11.2

**Audit criteria:**

Throughout the period in all material aspects:

Information necessary to easily identify and communicate with the single point of contact was:

- publicly available;
- easily accessible; and
- up to date.

**The following are certain operational benchmark(s) defined by the audited service:**

“single point of contact”:  
one mechanism to contact the audited service for help.

**Materiality threshold:**

If a control was not suitably designed and operated effectively to satisfy the obligation for at least 95% of the DSA Examination Period, and/or if there was an actual or projected error of more than 5% (or other material qualitative variance) during the DSA Examination Period related to the audit criteria.

**Audit procedures and information relied upon:**

In order to evaluate the audited service’s compliance with this DSA Specified Requirement, we performed substantive procedures, although controls existed, as outlined below:

1. Conducted a walkthrough and inquired with management to gain an understanding of the public facing website whereat Member States’ authorities, the Commission and the European Board for Digital Services can contact the audited service pursuant to Article 11, thus verifying that the audited service has designated a single point of contact that is easily identifiable and can be accessed directly from the audited service’s Home Page or mobile application using a clearly visible hyperlink or after navigating a reasonable number of menus.
2. Inspected the public facing website whereat Member States’ authorities, the Commission and the European Board for Digital Services can contact the service provider pursuant to Article 11, noting that the audited service designated a single point of contact that is publicly accessible without needing to log into the service. Reviewed additional supporting documentation including reviewing the inbox for receiving requests and the monitoring log to confirm that the single point of contact is kept up to date throughout the duration of the DSA Examination Period.
3. Inspected the single point of contact webpage throughout the DSA Examination Period and confirmed its existence.
4. Inquired with management and management noted that no significant changes were made to the policies, processes and/or controls after the walkthrough had been conducted through the end of the DSA Examination Period.


**Changes to the audit procedures during the audit:**

None.

**Results of procedures performed, how reasonable level of assurance was achieved, and conclusion:**

There were no material deviations identified in the performance of the above procedures, unless denoted below. The results of the audit procedures were deemed sufficient to obtain reasonable assurance.

**Positive** – In our opinion, the audited service complied with this DSA Specified Requirement during the DSA Examination Period in all material respects.

**Recommendations on specific measures:**

Not applicable.

**Recommended timeframe to implement specific measures:**

Not applicable.

<b>Obligation:</b>	<b>Audit criteria:</b>	<b>Materiality threshold:</b>
11.3	<p>Throughout the period in all material aspects:</p> <p>The official language or languages of the Member State that can be used to communicate with the single point of contact was:</p> <ul style="list-style-type: none"> <li>- specified within public information;</li> <li>- broadly understood by the largest possible number of Union citizens; and</li> <li>- included at least one of the official language(s) of the Member State in which the provider had its main establishment or where its legal representative resided.</li> </ul> <p><b>The following are certain operational benchmark(s) defined by the audited service:</b></p> <p>“single point of contact”: one mechanism to contact the audited service for help.</p>	<p>If a control was not suitably designed and operated effectively to satisfy the obligation for at least 95% of the DSA Examination Period, and/or if there was an actual or projected error of more than 5% (or other material qualitative variance) during the DSA Examination Period related to the audit criteria.</p>

**Audit procedures and information relied upon:**

In order to evaluate the audited service’s compliance with this DSA Specified Requirement, we performed substantive procedures, although controls existed, as outlined below:

1. Conducted a walkthrough and inquired with management and inspected the public facing website whereat Member States’ authorities, the Commission and the Board can contact the audited service pursuant to Article 11 to gain an understanding of the language(s) the single point of contact is presented in.



2. Inspected the single point of contact webpage and determined that the single point of contact is presented in English, which is an official language of Ireland (where the audited service has its main establishment) and is broadly understood by Union citizens as stated on the official European Union website.

3. Inquired with management and management noted that no significant changes were made to the policies, processes and/or controls after the walkthrough had been conducted through the end of the DSA Examination Period.

**Changes to the audit procedures during the audit:**

None.

**Results of procedures performed, how reasonable level of assurance was achieved, and conclusion:**

There were no material deviations identified in the performance of the above procedures, unless denoted below. The results of the audit procedures were deemed sufficient to obtain reasonable assurance.

**Positive** – In our opinion, the audited service complied with this DSA Specified Requirement during the DSA Examination Period, in all material respects.

**Recommendations on specific measures:**

Not applicable.

**Recommended timeframe to implement specific measures:**

Not applicable.

<b>Obligation:</b>	<b>Audit criteria:</b>	<b>Materiality threshold:</b>
12.1	<p>Throughout the period, in all material aspects:</p> <p>A single point of contact was designated for recipients of the service that enables the recipients to communicate directly and rapidly by electronic means, and in a user-friendly manner, with the designated point of contact. Recipients were able to choose the means of communication, which do not rely solely on automated tools.</p> <p><b>The following are certain operational benchmark(s) defined by the audited service:</b></p> <p>“communicate rapidly”: a service recipient can communicate rapidly when the required steps do not hinder submitting the communication.</p> <p>“single point of contact”: one mechanism to contact the audited service for help.</p>	<p>If a control was not suitably designed and operated effectively to satisfy the obligation for at least 95% of the DSA Examination Period, and/or if there was an actual or projected error of more than 5% (or other material qualitative variance) during the DSA Examination Period related to the audit criteria.</p>



### Audit procedures and information relied upon:

In order to evaluate the audited service's compliance with this DSA Specified Requirement, we performed substantive procedures, although controls existed, as outlined below:

1. Conducted a walkthrough and inquired with management to gain an understanding of the single point of contact and communication means.
2. Inspected the user journey flow provided by the audited service and independently reperformed the user journey flow on the audited service's web page and any other applicable user interface(s) during the DSA Examination Period from an EU IP address and sought help through each available communication option, and determined that there was a single point of contact designated for direct and rapid communication, the point of contact was conducted via electronic means and in a user-friendly manner, and the point of contact means did not rely solely on automated tools.
3. Inspected a sample of communications, sampled in accordance with the sampling approach described in Appendix 2, with the point of contact such as email correspondence and ticket notes and determined that the user inquiries submitted were responded to through non-automated tools.
4. Inquired with management and management noted that no significant changes were made to the policies, processes and/or controls after the walkthrough had been conducted through the end of the DSA Examination Period.

### Changes to the audit procedures during the audit:

None.

### Results of procedures performed, how reasonable level of assurance was achieved, and conclusion:

There were no material deviations identified in the performance of the above procedures, unless denoted below. The results of the audit procedures were deemed sufficient to obtain reasonable assurance.

**Positive** – In our opinion, the audited service complied with this DSA Specified Requirement during the DSA Examination Period, in all material respects.

### Recommendations on specific measures:

Not applicable.

### Recommended timeframe to implement specific measures:

Not applicable.

Obligation:	Audit criteria:	Materiality threshold:
12.2	<p>Throughout the period, in all material aspects:</p> <p>The information necessary for recipients of the service to easily identify their single point(s) of contact was:</p> <ul style="list-style-type: none"> <li>- made publicly available;</li> <li>- easily accessible; and</li> <li>- kept up to date.</li> </ul>	<p>If a control was not suitably designed and operated effectively to satisfy the obligation for at least 95% of the DSA Examination Period, and/or if there was an actual or projected error of more than 5% (or other material qualitative variance)</p>



	<p><b>The following are certain operational benchmark(s) defined by the audited service:</b></p> <p>“single point of contact”: one mechanism to contact the audited service for help.</p>	during the DSA Examination Period related to the audit criteria.
<p><b>Audit procedures and information relied upon:</b></p> <p>In order to evaluate the audited service’s compliance with this DSA Specified Requirement, we performed substantive procedures, although controls existed, as outlined below:</p> <ol style="list-style-type: none"> <li>1. Conducted a walkthrough and inquired with management including inspecting the procedures and results of the internal assessment that the audited service performed to gain an understanding of the single point of contact and the process to keep it up to date.</li> <li>2. Assessed the user journey flow during the DSA Examination Period on the audited service’s web page(s) and any other applicable user interface(s) and determined that the single point of contact is publicly available, is easily identifiable, and is easily accessible.</li> <li>3. Independently reperformed the user journey flow from an EU IP address throughout the DSA Examination Period and determined that the single point of contact was kept up to date.</li> <li>4. Inquired with management and management noted that no significant changes were made to the policies, processes and/or controls after the walkthrough had been conducted through the end of the DSA Examination Period.</li> </ol> <p><b>Changes to the audit procedures during the audit:</b></p> <p>None.</p> <p><b>Results of procedures performed, how reasonable level of assurance was achieved, and conclusion:</b></p> <p>There were no material deviations identified in the performance of the above procedures, unless denoted below. The results of the audit procedures were deemed sufficient to obtain reasonable assurance.</p> <p><b>Positive</b> – In our opinion, the audited service complied with this DSA Specified Requirement during the DSA Examination Period, in all material respects.</p>		
<p><b>Recommendations on specific measures:</b></p> <p>Not applicable.</p>		<p><b>Recommended timeframe to implement specific measures:</b></p> <p>Not applicable.</p>
<p><b>Obligation:</b></p> <p>14.1</p>	<p><b>Audit criteria:</b></p> <p>Throughout the period, in all material aspects:</p>	<p><b>Materiality threshold:</b></p> <p>If a control was not suitably designed and operated effectively to satisfy the</p>



	<p>1. The provider included information on any restrictions that they imposed in relation to the use of their service in respect of information provided by the recipients of the service, in their terms and conditions. The information included:</p> <ul style="list-style-type: none"> <li>- information on any policies, procedures, measures and tools used for the purpose of content moderation, including algorithmic decision-making and human review; and</li> <li>- rules of procedure of their internal complaint handling system.</li> </ul> <p>2. The information specified above was:</p> <ul style="list-style-type: none"> <li>- set out in clear, plain, intelligible, user-friendly and unambiguous language;</li> <li>- publicly available;</li> <li>- in an easily accessible; and</li> <li>- machine-readable format.</li> </ul> <p><b>Note:</b> The audited service's supplemental criteria for the scope of the audit were the terms of service and key policies that ensure the required transparency and enable recipients of the service to understand which content might be subject to moderation and enforcement on the audited service, pursuant to Article 14.</p> <p><b>The following are certain operational benchmark(s) defined by the audited service:</b></p> <p>"set out in clear, plain, intelligible, user-friendly and unambiguous language": the information is written and presented in a way that is easy for the intended audience to understand.</p> <p>"easily accessible and machine-readable format": the information or functionality is easy to find from the relevant interface.</p>	<p>obligation for at least 95% of the DSA Examination Period, and/or if there was an actual or projected error of more than 5% (or other material qualitative variance) during the DSA Examination Period related to the audit criteria.</p>
<p><b>Audit procedures and information relied upon:</b></p> <p>In order to evaluate the audited service's compliance with this DSA Specified Requirement, we performed substantive procedures, although controls existed, as outlined below:</p> <p>1. Conducted a walkthrough and inquired with management to gain an understanding of the policies and processes in place to determine how the audited service made available to the recipients of the service easily accessible and machine-readable terms and conditions (T&amp;Cs) written in clear, plain, intelligible, user-friendly, and unambiguous language and containing information regarding conditions for, and any restrictions on, the use of the service. Also,</p>		



inquired with management to determine how the information contained in the T&Cs included algorithmic decision-making and human review as well as the rules of procedure for their internal complaint handling system.

2. Assessed the design of the policies and processes in place during the DSA Examination Period were appropriate to comply with the DSA Specified Requirement.

3. Inspected the terms of service and key policies that ensure the required transparency and enable recipients of the service to understand which content might be subject to moderation and enforcement on the audited service, pursuant to Article 14 (In-Scope Terms) and determined that the In-Scope Terms:

- included information on restrictions that the audited service imposes on the use of the service, including information on algorithmic decision-making and human review, as well as the rules of procedure of their internal complaint handling system;

- were written in clear, plain, intelligible, user-friendly, and unambiguous language in accordance with the audited service's internal guidelines utilized by internal teams as a best practice for policy writing; and

- were publicly available, easily accessible to the recipients of the service, and in a machine-readable format.

4. Inquired with management and management noted that no significant changes were made to the policies, processes and/or controls after the walkthrough had been conducted through the end of the DSA Examination Period.

#### **Changes to the audit procedures during the audit:**

None.

#### **Results of procedures performed, how reasonable level of assurance was achieved, and conclusion:**

There were no material deviations identified in the performance of the above procedures, unless denoted below. The results of the audit procedures were deemed sufficient to obtain reasonable assurance.

**Positive** - In our opinion, the audited service complied with this DSA Specified Requirement during the DSA Examination Period, in all material respects.

#### **Recommendations on specific measures:**

Not applicable.

#### **Recommended timeframe to implement specific measures:**

Not applicable.

<b>Obligation:</b>	<b>Audit criteria:</b>	<b>Materiality threshold:</b>
14.2	<p>Throughout the period, in all material aspects:</p> <p>The provider informed recipients of any significant change to the terms and conditions of the service.</p>	<p>If a control was not suitably designed and operated effectively to satisfy the obligation for at least 95% of the DSA Examination Period, and/or if there was an actual or projected error of more than 5% (or other material qualitative variance)</p>





	<p><b>The following are certain operational benchmark(s) defined by the audited service:</b></p> <p>“significant change”: a significant change in a policy is defined as a change in policy language that would materially and noticeably impact or further restrict the usage, rights or responsibilities, or allow new forms of usage, rights or responsibilities, for a recipient of the service.</p>	<p>during the DSA Examination Period related to the audit criteria.</p>
<p><b>Audit procedures and information relied upon:</b></p> <p>In order to evaluate the audited service’s compliance with this DSA Specified Requirement, we evaluated the design and operation of controls and performed substantive procedures, as outlined below:</p> <ol style="list-style-type: none"> <li>1. Conducted a walkthrough and inquired with management to gain an understanding of the policies, and processes in place to determine how the audited service informed recipients of any significant change to the terms of service and key policies that ensure the required transparency and enable recipients of the service to understand which content might be subject to moderation and enforcement on the audited service pursuant to Article 14 (In-Scope Terms).</li> <li>2. Assessed the design of the policies and processes in place during the DSA Examination Period were appropriate to comply with the DSA Specified Requirement.</li> <li>3. Inspected the audited service's significant change policy and determined that it included definitions and illustrative examples of a “significant change”. Inspected a sample of changes made to In-Scope Terms during the DSA Examination Period, sampled in accordance with the sampling approach described in Appendix 2, and determined that the sample changes were appropriately assessed for significance in accordance with the audited service's internal policy. Inspected the public facing announcement pages and determined that the audited service informed recipients of the service of significant changes to In-Scope Terms, in all material respects.</li> <li>4. Inspected relevant IT controls, including controls related to change management and logical access, for the relevant systems in the production environment and determined that the controls were in place throughout the DSA Examination Period to address the key IT risks.</li> <li>5. Inquired with management and management noted that no significant changes were made to the policies, processes and/or controls after the walkthrough had been conducted through the end of the DSA Examination Period.</li> </ol> <p><b>Changes to the audit procedures during the audit:</b></p> <p>None.</p> <p><b>Results of procedures performed, how reasonable level of assurance was achieved, and conclusion:</b></p> <p>There were no material deviations identified in the performance of the above procedures, unless denoted below. The results of the audit procedures were deemed sufficient to obtain reasonable assurance.</p> <p><b>Positive</b> - In our opinion, the audited service complied with this DSA Specified Requirement during the DSA Examination Period, in all material respects.</p>		



<b>Recommendations on specific measures:</b>  Not applicable.	<b>Recommended timeframe to implement specific measures:</b>  Not applicable.
---	---

<b>Obligation:</b>  14.4	<b>Audit criteria:</b>  Throughout the period, in all material aspects:  The provider acted in a diligent, objective and proportionate manner in applying and enforcing the restrictions referred to in Article 14.1, with due regard to the rights and legitimate interests of all parties involved, including the fundamental rights of the recipients of the service, such as the freedom of expression, freedom and pluralism of the media, and other fundamental rights and freedoms as enshrined in the Charter.  <b>The following are certain operational benchmark(s) defined by the audited service:</b>  “diligent, objective and proportionate manner”: the audited service bases content decisions on policies that are non-arbitrary and objective, e.g. taking into account fundamental rights.	<b>Materiality threshold:</b>  If a control was not suitably designed and operated effectively to satisfy the obligation for at least 95% of the DSA Examination Period, and/or if there was an actual or projected error of more than 5% (or other material qualitative variance) during the DSA Examination Period related to the audit criteria.
--------------------------------	--	---

#### Audit procedures and information relied upon:

In order to evaluate the audited service’s compliance with this DSA Specified Requirement, we evaluated the design and operation of controls and performed substantive procedures, as outlined below:

1. Conducted a walkthrough and inquired with management to determine how the audited service acted in a diligent, objective, and proportionate manner in applying and enforcing restrictions referred to in Article 14.1.
2. Assessed the design of the policies and processes in place and determined that the policies and suite of controls were appropriately designed and operated in enabling the audited service to act in a diligent, objective, and proportionate manner in applying and enforcing the restrictions referred to in Article 14.1.
3. Inspected the 2024 Systemic Risk Assessment (SRA) documentation retained pursuant to Article 34 to determine how the audited service executed the 2024 SRA to ensure diligent, objective, and proportionate application and enforcement of terms and conditions, by assessing, with respect to the audited service, the risk of various prohibited content. The 2024 SRA included assessment of the following risk statements that specifically consider the diligent, objective and proportionate application and enforcement of terms and conditions:
  - Risk that a service removes content that does not constitute a necessary or proportionate removal of content with a legitimate purpose
  - Risk that users are not able to report potentially violating content on a service



<div><div>- Risk that users are not able to appeal content removals on a service</div><div>Per inspection of the 2024 SRA documentation, determined that it cited various instances of application and enforcement of restrictions applied by the audited service to demonstrate it is performed in a diligent, objective and proportionate manner.</div><div>4. Inquired with management, and for a sample content moderation system, sampled in accordance with the sampling approach described in Appendix 2, inspected system documentation, dashboards and reports and ascertained that the system performance and quality was monitored for the duration of the DSA Examination Period, and there were no significant changes in model performance based on pre-defined thresholds. Inspected system and process documentation and determined that a formal process was in place to investigate anomalies and update the model logic, if needed. Inspected change management policies, procedures and documentation and determined that the policies require segregation of duties for approval and implementation of any changes.</div><div>5. Inspected relevant IT controls, including controls related to change management and logical access, for the relevant systems in the production environment and determined that the controls were in place throughout the DSA Examination Period to address the key IT risks.</div><div>6. Inquired with management and management noted that no significant changes were made to the policies, processes and/or controls after the walkthrough had been conducted through the end of the DSA Examination Period.</div><div><b>Changes to the audit procedures during the audit:</b></div><div>None.</div><div><b>Results of procedures performed, how reasonable level of assurance was achieved, and conclusion:</b></div><div>There were no material deviations identified in the performance of the above procedures, unless denoted below. The results of the audit procedures were deemed sufficient to obtain reasonable assurance.</div><div><b>Positive</b> - In our opinion, the audited service complied with this DSA Specified Requirement during the DSA Examination Period, in all material respects.</div></div>		
<b>Recommendations on specific measures:</b>  Not applicable.		<b>Recommended timeframe to implement specific measures:</b>  Not applicable.
<b>Obligation:</b>  14.5	<b>Audit criteria:</b>  Throughout the period, in all material aspects:  1. The provider provided a summary of the terms and conditions of the services to the recipients of such services. The summary was: - concise; - easily accessible; - machine-readable; and	<b>Materiality threshold:</b>  If a control was not suitably designed and operated effectively to satisfy the obligation for at least 95% of the DSA Examination Period, and/or if there was an actual or projected error of more than 5% (or other material qualitative variance)



	<p>- in clear and unambiguous language.</p> <p>2. The summary included available remedies and redress mechanisms.</p> <p>The audited service's supplemental criteria for the scope of the audit were the terms of service and key policies that ensure the required transparency and enable recipients of the service to understand which content might be subject to moderation and enforcement on the audited service pursuant to Article 14.</p> <p><b>The following are certain operational benchmark(s) defined by the audited service:</b></p> <p>"concise, easily accessible and machine-readable": the information or functionality is easy to find from the relevant interface.</p> <p>"summary": a summary that is succinct and user-friendly, sets out the main topics covered and provides an easy means to access further information and navigate to the underlying topics. In this context, "user-friendly" means that the summary should be designed to make it easy for the relevant recipients of the service to explore the full range of relevant resources, for example by providing links and grouping relevant sections of the policy under easy-to-understand headings. "Succinct" means that the summary is a brief overview which allows recipients of the service to quickly understand the main topics and easily determine what topics are included in the document.</p> <p>"clear and unambiguous language": the information is written and presented in a way that is easy for the intended audience to understand.</p> <p>"main elements": in respect of terms of service and other contractual agreements governing the use of Google's products / services, "main elements" means the key topics covered by the terms of service which allow the recipient of the service to understand which conduct might be subject to moderation and enforcement on the audited service, the potential consequences for engaging in violative conduct and remedies and redress mechanisms.</p> <p>In respect of key policies, "main elements" means the different categories of content, practices and behavior</p>	<p>during the DSA Examination Period related to the audit criteria.</p>
--	---	---



	that are subject to moderation on the audited service, together with any category-specific information on enforcement action and appeals / means of redress.	
<p><b>Audit procedures and information relied upon:</b></p> <p>In order to evaluate the audited service's compliance with this DSA Specified Requirement, we evaluated the design and operation of controls and performed substantive procedures, as outlined below:</p> <ol style="list-style-type: none"> <li>1. Conducted a walkthrough and inquired with management to gain an understanding of how the audited service made available to the recipients of the service a concise, easily accessible, and machine-readable summary of the terms of service and key policies that ensure the required transparency and enable recipients of the service to understand which content might be subject to moderation and enforcement pursuant to Article 14 (In-Scope Terms) that included the main elements of the In-Scope Terms, including the available remedies and redress mechanisms.</li> <li>2. Assessed the design of the policies and processes in place during the DSA Examination Period were appropriate to comply with the DSA Specified Requirement.</li> <li>3. Inspected the audited service's In-Scope Terms and determined that a concise, easily accessible, and machine-readable summary was available that addressed the main elements of In-Scope Terms, including available remedies and redress mechanisms, in clear and unambiguous language.</li> <li>4. Inspected relevant IT controls, including controls related to change management and logical access, for the relevant systems in the production environment, and determined that the controls were in place throughout the DSA Examination Period to address the key IT risks.</li> <li>5. Inquired with management and management noted that no significant changes were made to the policies, processes and/or controls after the walkthrough had been conducted through the end of the DSA Examination Period.</li> </ol> <p><b>Changes to the audit procedures during the audit:</b></p> <p>None.</p> <p><b>Results of procedures performed, how reasonable level of assurance was achieved, and conclusion:</b></p> <p>There were no material deviations identified in the performance of the above procedures, unless denoted below. The results of the audit procedures were deemed sufficient to obtain reasonable assurance.</p> <p><b>Positive</b> - In our opinion, the audited service complied with this DSA Specified Requirement during the DSA Examination Period, in all material respects.</p>		
<p><b>Recommendations on specific measures:</b></p> <p>Not applicable.</p>	<p><b>Recommended timeframe to implement specific measures:</b></p> <p>Not applicable.</p>	



<b>Obligation:</b>	<b>Audit criteria:</b>	<b>Materiality threshold:</b>
14.6	<p>Throughout the period, in all material aspects:</p> <p>The provider published their terms and conditions in the official languages of all the Member States in which they offer their services.</p> <p><b>The following are certain operational benchmark(s) defined by the audited service:</b></p> <p>“official languages”: the 24 official languages of the Union: Bulgarian, Croatian, Czech, Danish, Dutch, English, Estonian, Finnish, French, German, Greek, Hungarian, Gaelic, Italian, Latvian, Lithuanian, Maltese, Polish, Portuguese, Romanian, Slovak, Slovenian, Spanish and Swedish.</p>	<p>If a control was not suitably designed and operated effectively to satisfy the obligation for at least 95% of the DSA Examination Period, and/or if there was an actual or projected error of more than 5% (or other material qualitative variance) during the DSA Examination Period related to the audit criteria.</p>
<p><b>Audit procedures and information relied upon:</b></p> <p>In order to evaluate the audited service’s compliance with this DSA Specified Requirement, we evaluated the design and operation of controls and performed substantive procedures, as outlined below:</p> <ol style="list-style-type: none"> <li>1. Conducted a walkthrough and inquired with management to gain an understanding as to how the audited service published their terms of service and key policies that ensure the required transparency and enable recipients of the service to understand which content might be subject to moderation and enforcement pursuant to Article 14 (In-Scope Terms) in the official languages of all the Member States in which they offer their services.</li> <li>2. Assessed the design of the policies and processes in place during the DSA Examination Period were appropriate to comply with the DSA Specified Requirement.</li> <li>3. Inspected the audited service's In-Scope Terms to determine if In-Scope Terms were publicly available in all 24 official languages of the Member States.</li> </ol> <p>From 1 June 2024 to 5 November 2024, the "Community Guidelines for user generated content on Search" (previously known as the Policy for Content Posted by Users on Search) was not available in seven official languages of the Member States. From 6 November 2024 to 31 May 2025, the "Community Guidelines for user generated content on Search" was available in all 24 official languages of the Member States. Tested the updated "Community Guidelines for user generated content on Search" and determined that, for the period from 6 November 2024 to 31 May 2025, the audited service complied with this DSA Specified Requirement.</p> <ol style="list-style-type: none"> <li>4. Inspected relevant IT controls, including controls related to change management and logical access, for the relevant systems in the production environment and determined that the controls were in place throughout the DSA Examination Period to address the key IT risks.</li> <li>5. Inquired with management and management noted that no significant changes were made to the policies, processes and/or controls after the walkthrough had been conducted through the end of the DSA Examination Period.</li> </ol>		


**Changes to the audit procedures during the audit:**

None.

**Results of procedures performed, how reasonable level of assurance was achieved, and conclusion:**

There were no material deviations identified in the performance of the above procedures, unless denoted below. The results of the audit procedures were deemed sufficient to obtain reasonable assurance.

**Negative** – In our opinion, except for the effects of the material noncompliance described in the following paragraph, the audited service complied with this DSA Specified Requirement during the DSA Examination Period, in all material respects.

From 1 June 2024 to 5 November 2024, the "Community Guidelines for user generated content on Search" (previously known as the Policy for Content Posted by Users on Search) was not available in seven official languages of the Member States.

From 6 November 2024 to 31 May 2025, the "Community Guidelines for user generated content on Search" was available in all 24 official languages of the Member States. Tested the updated "Community Guidelines for user generated content on Search" and determined that, for the period from 6 November 2024 to 31 May 2025, the audited service complied with this DSA Specified Requirement.

**Recommendations on specific measures:**

Not applicable.

**Recommended timeframe to implement specific measures:**

Not applicable.

<b>Obligation:</b>	<b>Audit criteria:</b>	<b>Materiality threshold:</b>
15.1	<p>Throughout the period, in all material aspects:</p> <ol style="list-style-type: none"> <li>1. The provider published at least one transparency report on content moderation that they engaged in during the relevant period.</li> <li>2. The published transparency report(s) meet the following criteria: <ul style="list-style-type: none"> <li>- in a machine-readable format;</li> <li>- easily accessible; and</li> <li>- clear and easily comprehensible.</li> </ul> </li> <li>3. The provider has included in the published transparency reports, information enumerated in points (a) to (e) of Article 15.1, summarized as follows:</li> </ol>	<p>If a control was not suitably designed and operated effectively to satisfy the obligation for at least 95% of the DSA Examination Period, and/or if there was an actual or projected error of more than 5% (or other material qualitative variance) during the DSA Examination Period related to the audit criteria.</p>





	<p>(a) information / metrics on orders received from Member States' authorities (including Article 9 and 10 orders) which are categorized by:</p> <ul style="list-style-type: none"> <li>(i) type of illegal content,</li> <li>(ii) the Member State issuing the order, and</li> <li>(iii) median time needed to inform authorities of its receipt and to give effect to the order;</li> </ul> <p>(b) information / metrics on notices submitted in accordance with Article 16 (for hosting services only - Not applicable for Google Search);</p> <p>(c) information / metrics on content moderation at the provider's own initiative;</p> <p>(d) information / metrics on complaints received through internal complaint-handling systems (additional information for online platforms in accordance with Article 20 - Not applicable for Google Search), and</p> <p>(e) information / metrics on the use of automated means for content moderation.</p>	
--	--	--

#### **Audit procedures and information relied upon:**

In order to evaluate the audited service's compliance with this DSA Specified Requirement we evaluated the design and operation of controls and performed substantive procedures, as outlined below:

1. Conducted a walkthrough and inquired with management to gain an understanding of how the Trust & Safety team consolidates content moderation narratives and metrics from the audited service, cross-functional and Safety Data Platform (SDP) teams into the draft transparency report, obtains necessary approvals, and converts the narratives and metrics into a format suitable for publication. Determined that verification checks on scripts used to transfer the metrics from the source data to the DSA Dashboard and metrics provided by the audited service and cross-functional team for use in the transparency reports are documented in a Metric Validation Scorecard.
2. Inspected the Google Transparency Report PDF Download Centre for the published Transparency Reports, noting that they were presented in the necessary format, clear, comprehensible, and easily accessible. Verified that the transparency reports were published at least every six months with the transparency reports being published on 28 August 2024 and 28 February 2025. Confirmed that the reports during the DSA Examination Period were published in English, in a machine-readable PDF format and included content moderation information.
3. Inspected evidence of individuals who published the transparency report and determined that these individuals were appropriately included in the authorized group for publishing based on their job title/function.
4. Inspected the published (EU DSA) Biannual VLOSE/VLOP Transparency Reports published on 28 August 2024 and 28 February 2025 from the Google Transparency Report PDF Download Centre, performed a comparative analysis against the requirement outlined in points (a) to (e) of Article 15.1 and verified that each report included the applicable required information based on the type of provider. Inspected evidence of reviews performed by stakeholders who validated that the information enumerated in points (a) to (e) of Article 15.1 was included in the transparency report.





5. Inspected a list of job titles of stakeholders provided by the audited service and matched against the review and approval screenshots for the published transparency reports. Validated that all approving stakeholders were appropriate based on their job functions/titles.
6. Inspected the validation review document completed by the audited service to ensure the source data was extracted completely and accurately to the DSA Dashboard. Inspected a copy of the DSA Dashboard along with the published transparency report and determined that the data per the DSA Dashboard aligns completely and accurately with the published transparency report.
7. Inspected the published transparency reports for disclosures related to the use of automated means for content moderation and determined that the testing performed for other Articles did not contradict the information within the published transparency reports. Inquired with management and for a sample content moderation system, sampled in accordance with the sampling approach described in Appendix 2, inspected system documentation, dashboards and reports and ascertained that the system performance and quality was monitored for the duration of the DSA Examination Period, and there were no significant changes in model performance based on pre-defined thresholds. Inspected system and process documentation and determined that a formal process is in place to investigate anomalies and update the model logic, if needed. Inspected change management policies, procedures and documentation and determined that the policies require segregation of duties for approval and implementation of any changes.
8. Inspected relevant IT controls, including controls related to change management and logical access, for the relevant systems in the production environment, and determined that the controls were in place throughout the DSA Examination Period to address key IT risks.
9. Inquired with management and management noted that no significant changes were made to the policies, processes and/or controls after the walkthrough had been conducted through the end of the DSA Examination Period.

**Changes to the audit procedures during the audit:**

None.

**Results of procedures performed, how reasonable level of assurance was achieved, and conclusion:**

There were no material deviations identified in the performance of the above procedures, unless denoted below. The results of the audit procedures were deemed sufficient to obtain reasonable assurance.

**Positive** - In our opinion, the audited service complied with this DSA Specified Requirement during the DSA Examination Period, in all material respects.

**Recommendations on specific measures:**

Not applicable.

**Recommended timeframe to implement specific measures:**

Not applicable.

**Section 2 — Additional provisions applicable to providers of hosting services, including online platforms – Not applicable**



### Section 3 — Additional provisions applicable to providers of online platforms

Obligation:	Audit criteria:	Materiality threshold:
24.2	<p>Throughout the period, in all material aspects:</p> <ol style="list-style-type: none"> <li>1. The provider published information on the average monthly active recipients of the service in the Union.</li> <li>2. The information above was published in a publicly available section of their online interface.</li> <li>3. The information referenced above was published by 17 February 2023 and at least once every six months thereafter.</li> <li>4. The average monthly active recipients were calculated as an average over the period of the prior six months.</li> </ol> <p><b>The following are certain operational benchmark(s) defined by the audited service:</b></p> <p>“monthly active recipient”: signed in or signed out recipients, who are in the EU and have engaged at least once per 28 days/month on any surface where recipients can interact with the service (e.g. mobile, tablet, browser, etc.) and as further explained in the Overview and Additional Notes section of the MAR reports.</p>	<p>If a control was not suitably designed and operated effectively to satisfy the obligation for at least 95% of the DSA Examination Period, and/or if there was an actual or projected error of more than 5% (or other material qualitative variance) during the DSA Examination Period related to the audit criteria.</p>
<p><b>Audit procedures and information relied upon:</b></p> <p>In order to evaluate the audited service’s compliance with this DSA Specified Requirement, we evaluated the design and operation of controls and performed substantive procedures, as outlined below:</p> <ol style="list-style-type: none"> <li>1. Conducted a walkthrough and inquired with management to gain an understanding of the process used for determining signed-in and signed-out recipients and the process for performing metric validation procedures prior to publication of the Monthly Active Recipients (MAR) Reports and the publication process of the MAR Reports to the Google Transparency Report PDF Download Centre.</li> <li>2. Inspected the Google Transparency Report PDF Download Centre and confirmed that the MAR Reports were published at least every 6 months, with the MAR Reports being published on 16 August 2024 and 14 February 2025 during the DSA Examination Period.</li> </ol>		



3. Inspected the MAR Reports published during the DSA Examination Period and validated that these Reports contained information on the average monthly active recipients as laid out under the DSA Specified Requirements and were published in a publicly available section of the audited provider's online interface.
4. Inspected methodology used for calculating the average monthly active recipients of the service in the Union and validated through reperformance of the calculations that the information is calculated as an average over a period of the past six months.
5. Inspected the Metric Validation Scorecard and the related tickets for approvals and confirmed that all of the metrics published in the MAR Reports during the DSA Examination Period have been validated by the Trust & Safety team, including a verification of the script used to pull recipient count data for each in-scope audited service from the correct data sources. Verified that the scorecard review was completed prior to report publication via inspection of all stakeholder approval dates. Validated that all approving stakeholders were appropriate based on their job functions/titles.
6. Inspected user access lists and confirmed the employees that have access to modify the scripts to pull monthly active recipient data for each in-scope audited service are appropriate based on their job title/function.
7. Inspected relevant IT controls, including controls related to change management and logical access, for the relevant systems in the production environment and determined that the controls were in place throughout the DSA Examination Period to address key IT risks.
8. Inspected evidence of individuals who published the transparency report and determined that these individuals were appropriately included in the authorized group for publishing based on their job title/function.
9. Inquired with management and management noted that no significant changes were made to the policies, processes and/or controls after the walkthrough had been conducted through the end of the DSA Examination Period.

**Changes to the audit procedures during the audit:**

None.

**Results of procedures performed, how reasonable level of assurance was achieved, and conclusion:**

There were no material deviations identified in the performance of the above procedures, unless denoted below. The results of the audit procedures were deemed sufficient to obtain reasonable assurance.

**Positive** – In our opinion, the audited service complied with this DSA Specified Requirement during the DSA Examination Period, in all material respects.

**Recommendations on specific measures:**

Not applicable.

**Recommended timeframe to implement specific measures:**

Not applicable.



Obligation:	Audit criteria:	Materiality threshold:
24.3	<p>Throughout the period, in all material aspects:</p> <ol style="list-style-type: none"> <li>1. Upon request from the Digital Services Coordinator and/or the Commission, the provider communicated without undue delay the information on the average monthly active recipients of the service in the Union referred to in Article 24.2, updated to the moment of such request.</li> <li>2. The provider provided the following information upon request by the Digital Services Coordinator and/or the Commission: <ul style="list-style-type: none"> <li>- additional information on the calculation of the average monthly active recipients of the service in the Union referred to in Article 24.2, and</li> <li>- explanations and substantiations in respect of the data used.</li> </ul> </li> <li>3. The information provided to the Digital Services Coordinator and/or the Commission did not contain personal data.</li> </ol>	<p>If a control was not suitably designed and operated effectively to satisfy the obligation for at least 95% of the DSA Examination Period, and/or if there was an actual or projected error of more than 5% (or other material qualitative variance) during the DSA Examination Period related to the audit criteria.</p>
<p><b>Audit procedures and information relied upon:</b></p> <p>In order to evaluate the audited service's compliance with this DSA Specified Requirement, we evaluated the design and operation of controls and performed substantive procedures, as outlined below:</p> <ol style="list-style-type: none"> <li>1. Conducted a walkthrough and inquired with management to gain an understanding of the process for monitoring and recording all requests for information from the Digital Services Coordinator and/or the Commission by inquiring with the Independent Compliance Function (ICF) team. Determined that there have been no cases of requests for additional information on average monthly active recipients (MAR) data from the Digital Services Coordinator (DSC) and/or the Commission within the DSA Examination Period. Noted that the audited service has processes in place for monitoring and responding to these requests, such as the ICF mailbox pursuant to Article 41 which captures emails from the DSC and/or the Commission, and a system-generated log pursuant to Article 11 which tracks all DSA Point of Contact (POC) requests.</li> <li>2. Inspected screenshots of the ICF mailbox and DSA POC monitoring log pursuant to Article 11 and confirmed no requests were submitted by the Digital Services Coordinator and/or the Commission related to providing the calculation of the average MAR of the service in the Union and explanations with substantiations in respect of the data used.</li> <li>3. Inspected MAR data recipient files which were maintained at a product-specific level and noted that these were aggregate counts with no personal data. Determined that the audited service has policies in place to redact and remove Personally Identifiable Information, where applicable, from MAR report related requests received from the DSC and/or the Commission.</li> </ol>		



4. Inquired with management and management noted that no significant changes were made to the policies, processes and/or controls after the walkthrough had been conducted through the end of the DSA Examination Period.

**Changes to the audit procedures during the audit:**

None.

**Results of procedures performed, how reasonable level of assurance was achieved, and conclusion:**

There were no material deviations identified in the performance of the above procedures, unless denoted below. The results of the audit procedures were deemed sufficient to obtain reasonable assurance.

**Positive** – In our opinion, the audited service complied with this DSA Specified Requirement during the DSA Examination Period, in all material respects.

**Recommendations on specific measures:**

Not applicable.

**Recommended timeframe to implement specific measures:**

Not applicable.

**Section 4 — Additional provisions applicable to providers of online platforms allowing consumers to conclude distance contracts with traders - Not applicable**

**Section 5 — Additional obligations for providers of very large online platforms and of very large online search engines to manage systemic risks**

Obligation:	Audit criteria:	Materiality threshold:
34.1	<p>Throughout the period, in all material aspects:</p> <ol style="list-style-type: none"> <li>1. Systemic risks in the Union stemming from the design or functioning of the provider's service and its related systems, including algorithmic systems, or from the use made of the provider's services are diligently identified, analyzed and assessed (the "risk assessment").</li> <li>2. The risk assessment was carried out at least once every year after 28 August 2023.</li> <li>3. Risk assessments were carried out prior to deploying functionalities that are likely to have a critical impact on the risks identified pursuant to this article if such functionalities were deployed.</li> </ol>	<p>If a control was not suitably designed and operated effectively to satisfy the obligation for at least 95% of the DSA Examination Period, and/or if there was an actual or projected error of more than 5% (or other material qualitative variance) during the DSA Examination Period related to any of the audit criteria.</p>



	<p>4. The risk assessment was specific to the provider's services.</p> <p>5. The risk assessment was proportionate to the systemic risks.</p> <p>6. The risk assessment considered the severity and probability of the identified risks.</p> <p>7. The risk assessment included the systemic risks specified within Article 34.1.</p> <p><b>Note:</b> The audit criteria is supplemented by any additional provisions as outlined in Article 13 of the Delegated Regulation.</p> <p><b>The following are certain operational benchmark(s) defined by the audited service:</b></p> <p>"diligently identify, analyze and assess any systemic risks":</p> <p>the audited service's SRA Playbook outlines the comprehensive methodology, detailing how the audited service diligently identifies, analyzes, and assesses any systemic risks.</p>	
<p><b>Audit procedures and information relied upon:</b></p> <p>In order to evaluate the audited service's compliance with this DSA Specified Requirement, we evaluated the design and operation of controls and performed substantive procedures, as outlined below:</p> <ol style="list-style-type: none"> <li>1. Conducted a walkthrough and inquired with management to gain an understanding of the audited service's Systemic Risk Assessment (SRA) methodology and process, and how it aligns with the requirements of the DSA.</li> <li>2. Assessed the design of the policies, processes, and controls in place to evaluate the audited service's compliance with this DSA Specified Requirement.</li> </ol> <p>Inspected the audited service's SRA Playbook and determined that the audited service's methodology and process for performing the risk assessment was designed appropriately and aligned with the regulatory requirements of the DSA. Inspected the SRA Playbook and determined that the 2024 SRA process and methodology was formally reviewed by relevant stakeholders before the 2024 SRA process was conducted and subsequently after the completion of the SRA, as indicated through sign-offs documented within the 2024 SRA Playbook.</p> <p>Inspected the 2024 SRA documentation for the audited service and determined that the audited service had conducted a risk assessment that was specific to the audited service and included assessment of a list of risk statements inclusive of systemic risks specified within Article 34.1. Inspected the 2024 SRA documentation and determined that the risk assessment conducted was proportionate to the systemic risks, by taking into consideration the severity and</p>		



probability for each risk statement, which was assessed in accordance with the methodology defined in the SRA Playbook.

Inspected the 2024 SRA documentation for the audited service and determined that it included a summary of insights gathered from external stakeholders that were relevant to the inclusion of certain risk statements. Inspected the 2024 SRA documentation and determined that external sources of information from various parties were leveraged in performing the assessment of the audited service's inherent and residual risks. As such, determined that the audited service has considered the external stakeholder insights to make decisions on the severity and probability risk rating for the systemic risks.

Inspected the weekly Independent Compliance Function (ICF) meeting agenda and excerpts of minutes of quarterly board meetings which demonstrate the procedures performed by the (ICF) during its independent 2024 SRA assessment and determined that the ICF assessed that the risks referred to in Article 34 were identified and properly reported on.

Inspected training materials and determined the ICF maintains and distributes the training materials to management and employees of the audited service to inform them of relevant obligations under the DSA.

Inspected the compliance monitoring plan and determined the ICF has a process to monitor the compliance of the audited service with its obligations under the DSA through performing internal controls validation and validation of completed remediations. To corroborate the aforementioned procedures performed by the ICF, inquired with the head compliance officer and confirmed that the ICF actively monitored the audited service's compliance with its obligations under the DSA, throughout the DSA Examination Period. Additionally, inspected the agendas and excerpts of meeting minutes of quarterly board meetings and ad hoc meetings, and determined the compliance monitoring plan has been reviewed and approved by the management body, and ICF provided status updates on the control validation process to demonstrate their monitoring of the compliance of the audited service with its obligations.

To assess the involvement of the management body of the audited provider in decisions related to risk management pursuant to Article 41.6 and 41.7, inspected meeting agenda and excerpts of minutes and determined that the results of the independent 2024 SRA assessment performed by the ICF were presented to the management body and 2024 SRA team during the DSA Examination Period.

Inspected meeting agendas and excerpt of the quarterly board meeting minutes and ad hoc meetings and determined that the management body devoted sufficient time to the consideration of the measures related to risk management, maintained active involvement in the decisions related to risk management, and ensured that adequate resources were allocated to the management of the risks identified in accordance with Article 34 as part of the ICF's independent 2024 SRA assessment. Evaluated the sufficiency of time devoted by the management body considering the ad hoc meetings scheduled between the compliance function and management body throughout the DSA Examination Period, in addition to their regular quarterly board meetings, which we determined were reasonable. To corroborate the aforementioned procedures performed by the management body, inquired with the management board and confirmed that the management body devoted sufficient time during the scheduled board meetings to DSA risk management decisions and processes and was actively involved in the decisions related to risk management.

3. Inspected the 2024 SRAs in order to assess how the audited service analyzed and assessed each risk, including how probability and severity of the risks were considered.

Inspected the 2024 SRA documentation and SRA Playbook to obtain an understanding of the audited service's description of the process to develop its risk statements and map risk statements for the audited service. Inspected the 2024 SRA documentation for the risks applicable to the audited service and performed additional inquiries with the audited service and obtained a rationale for each risk statement that was deemed not applicable for the audited





service. Assessed the rationale for each risk statement and determined that the risks applicable to the audited service were appropriately identified, based on the four categories of risks outlined within Recitals 80 - 83.

Inspected the scoring criteria, thresholds, and rationale for the probability and severity associated with each risk documented within the 2024 SRA documentation for the audited service, and where required, performed additional inquiries with the audited service to understand the rationale to support the risk assessment documented. Based on this analysis performed, determined that the assessment was appropriate, in accordance with Recital 79.

Inquired with management and determined that external insights were relied on for the purposes of supporting the scoring and evaluation of inherent risks and residual risks. Inspected the summary of insights and meeting summaries/outputs related to sources of these insights, including workshops and a non-exhaustive list of its engagement with safety expert organizations and institutions to assess the sources of information used, means of collection, whether and how the audited service relied on these scientific and technical insights, and determined that these insights were incorporated into the following aspects of the SRA:

1. Content of Risk statement: insights considered to evaluate the consistency of the risk statements with industry definitions and standards
2. Analysis for Scope, Remediability, Probability, and/or Preparedness: insights incorporated in the scoring of "Inherent risk" and "Residual Risk"
3. Product-Area (PA) Specific Considerations: insights considered for specific PA based on the relevance of the risk statements.

Inquired with management to understand whether and how the audited service tested assumptions on risks with groups most impacted by the specific risks. Upon inquiry, determined that the audited service conducted workshops with subject matter experts and stakeholders to test assumptions (i.e., pressure test positions used in the identification or analysis of risk statements) by comparing internal stakeholder insights to external stakeholder insights. Selected a sample of expert organizations and institutions that the audited service engaged with, sampled in accordance with the sampling approach described in Appendix 2, and inspected meeting invites, attendance records of participating organizations at the audited service hosted summits and events, and published blog articles summarizing the events. Based on inspection of this evidence, determined that it demonstrated "whether and how" the audited service tested assumptions with groups most impacted by the specific risk for the audited service.

Inquired with management to gain an understanding of the timeline of the risk assessment process. Inspected email communications and determined that the 2024 SRA documentation was submitted to the Commission on 28 August 2024, thus meeting the requirement of performing the risk assessment at least annually from 28 August 2023 onwards.

Inquired with management to gain an understanding of the process for conducting risk assessments for functionalities deployed during the DSA Examination Period that might have a critical impact on the systemic risks. Inspected the documented policy and determined that the policy defined the criteria to be used to identify a functionality that could have a critical impact on the systemic risk. The policy additionally outlined the process to confirm applicability of the requirement and conduct a risk assessment before the functionality is deployed. The policy document also identifies the roles of the stakeholders involved in the process. To address an audit recommendation from prior year, the audited service expanded the training on the policy defining the threshold for an off-cycle risk assessment by (1) establishing a dedicated distribution channel, (2) updating training content to streamline how stakeholders can identify and escalate launches that may trigger the off-cycle assessment process, and (3) ensuring 24/7 access to the training resources for all employees. Inspected the off-cycle risk assessment template and determined that the template prescribed the information to be documented for the off-cycle risk assessments, including a description of the functionality to be





deployed, a description of the effect on the severity and probability to the systemic risks, and a description of the existing or planned mitigations to address the risks.

Inquired with management and inspected the audited service's off-cycle risk assessment monitoring tracker and determined that there was one functionality deployed during the DSA Examination Period that was deemed to have a critical impact on the systemic risks. Inspected the off-cycle risk assessment template completed for the identified functionality and determined that the assessment was documented in the formalized off-cycle risk assessment template, reviewed and approved by relevant stakeholders and completed prior to the deployment of the functionality.

Selected a sample of functionalities deployed during the DSA Examination Period, sampled in accordance with the sampling approach described in Appendix 2, and performed inquiries with management to obtain an understanding of the nature of each sampled functionality. Based on the rationale provided, determined that it was appropriate that the sampled functionalities deployed did not meet the criteria to trigger an off-cycle risk assessment prior to deployment.

Inspected the 'Report of Systemic Risk Assessments' released by the audited service, and its underlying documentation, to determine adequate comprehensiveness of actions taken and adequacy of information in support of the assessment carried out pursuant to this article. The inspection included, but was not limited to, the following elements:

- (a) Reviewed the reports on risk assessment and risk mitigation for the relevant DSA Examination Period prepared by the audited service along with the supporting documents.
- (b) Evaluated information submitted by the audited service pursuant to Article 5 of the Delegated Regulation on the performance of audits, verifying its relevance and accuracy in the context of the risk assessment.
- (c) Analyzed all relevant transparency reports of the audited provider referred to in Article 15.1 to assess the audited service's disclosure and transparency regarding the risk assessment.
- (d) Assessed other relevant evidence (including test results, documentation, and statements made in response to written or oral questions) provided by the audited provider to ensure a thorough understanding of the risk assessment.
- (e) Assessed reports referred to in Article 35.2 of Regulation (EU) 2022/2065 and guidance from the Commission, including guidelines issued pursuant to Article 35.3 of that Regulation and any other relevant guidance issued by the Commission with respect to the application of Regulation (EU) 2022/2065 to confirm inclusion in the risk assessment.

Inquired with management and determined that no other risk assessment reports were considered relevant in support of the assessment carried out pursuant to this article.

Inquired with management, and for a sample content moderation system, sampled in accordance with the sampling approach described in Appendix 2, inspected system documentation, dashboards and reports and ascertained that the system performance and quality was monitored for the duration of the DSA Examination Period, and there were no significant changes in model performance based on pre-defined thresholds. Inspected system and process documentation and determined that a formal process is in place to investigate anomalies and update the model logic, if needed. Inspected change management policies, procedures and documentation and determined that the policies require segregation of duties for approval and implementation of any changes.

Inquired with management throughout the DSA Examination Period and inspected an infrastructure supporting the recommender system architecture which supports the recommendations made on all VLOPs and VLOSE and process documentation related to that recommender system architecture and determined that it was managed using a combination of common system workflows and tools. Inspected the recommender system architecture model



documentation and code and determined that the system functionality did not change significantly throughout the DSA Examination Period. Inspected system code and documentation evidence and determined that the user's preference and selection is used as input by the recommender system. Inspected system documentation, dashboards and reports and determined that the system performance and quality was monitored for the duration of the DSA Examination Period, and there were no significant changes in model performance based on pre-defined thresholds.

4. Inspected relevant IT controls, including controls related to change management and logical access, for the relevant systems in the production environment and determined that the controls were in place throughout the DSA Examination Period to address key IT risks.

5. Inquired with management and management noted that no significant changes were made to the policies, processes and/or controls after the walkthrough had been conducted through the end of the DSA Examination Period.

#### **Changes to the audit procedures during the audit:**

None.

#### **Results of procedures performed, how reasonable level of assurance was achieved, and conclusion:**

There were no material deviations identified in the performance of the above procedures, unless denoted below. The results of the audit procedures were deemed sufficient to obtain reasonable assurance.

**Positive with comments** - In our opinion, the audited service complied with this DSA Specified Requirement during the DSA Examination Period, in all material respects.

See below Recommendation on specific measures.

#### **Recommendations on specific measures:**

- (a) Pursuant to Article 34.1, as a recommended enhancement to the risk assessment process, the audited service should enhance the documentation of the relevant considerations that support its scoring rationale and include sufficient information to support reperformance of risk rating as part of audit testing.
- (b) Pursuant to Article 34.1, as a recommended enhancement to future off-cycle risk assessments, to ensure the risk assessment is appropriately conducted, the off-cycle assessment template should state whether the functionality impacted overall inherent risk or preparedness for the audited service.
- (c) Pursuant to Article 34.1, as a recommended enhancement to the risk assessment process, the audited service should revise the wording of the following risk statements to clearly reflect the intended scope that the risk statement is applicable for the current assessment cycle (i.e. that it is applicable to applications available on the VLOP/VLOSE rather than the VLOP/VLOSE itself):

#### **Recommended timeframe to implement specific measures:**

- (a) 30 September 2024 - 28 August 2025
- (b) 28 August 2025 - 28 February 2026
- (c) 28 August 2025 - 28 February 2026



<div>1. "Risk that an application or service does not perform equitably for children with varied learning styles, learning challenges, or disabilities"</div> <div>2. "Risk that an application or service primarily directed at or predominantly used by children is not of adequate quality across languages, markets, and age groups and has adverse impacts on children"</div> <div>3. "Risk that an application or service is not of adequate quality across languages, markets, and age groups"</div>		
<div>Obligation:</div> <div>34.2</div>	<div>Audit criteria:</div> <div>Throughout the period, in all material aspects:</div> <div><div>1. The risk assessment conducted considered whether and how the five factors specified in Article 34.2 influenced any of the systemic risks referred to in Article 34.1.</div><div>2. The risk assessment included an analysis of whether and how the risks specified in Article 34.1 are influenced by intentional manipulation of their service by inauthentic use or automated exploitation of the service.</div><div>3. The risk assessment included an analysis of whether and how the risks specified in Article 34.1 are influenced by intentional manipulation of their service by the amplification and potentially rapid and wide dissemination of illegal content.</div><div>4. The risk assessment includes an analysis of whether and how the risks specified in Article 34.1 are influenced by intentional manipulation of their service by the amplification and potentially rapid and wide dissemination of information that is incompatible with their terms and conditions.</div><div>5. The risk assessment considered specific regional or linguistic aspects, including when specific to a Member State.</div></div> <div><div>Note:</div><div>The audit criteria is supplemented by any additional provisions as outlined in Article 13 of the Delegated Regulation.</div></div>	<div>Materiality threshold:</div> <div>If a control was not suitably designed and operated effectively to satisfy the obligation for at least 95% of the DSA Examination Period, and/or if there was an actual or projected error of more than 5% (or other material qualitative variance) during the DSA Examination Period related to the audit criteria.</div>



### Audit procedures and information relied upon:

In order to evaluate the audited service's compliance with this DSA Specified Requirement, we evaluated the design and operation of controls and performed substantive procedures, as outlined below:

1. Conducted a walkthrough and inquired with management to gain an understanding of the audited service's Systemic Risk Assessment (SRA) methodology and process, and how it aligns with the requirements of the DSA.
2. Assessed the policies, processes, and controls in place, to evaluate the audited service's compliance with this DSA Specified Requirement.

Inspected the audited service's SRA Playbook and determined that the audited service's methodology and process for performing the risk assessment was designed appropriately and aligned with the regulatory requirements of the DSA. Inspected the 2024 SRA documented for the audited service and determined that the risk assessments included considerations for how the five factors specified in Article 34.2 influenced any of the systemic risks referred to in Article 34.1.

3. Inspected the list of "risk factors" and "non-exhaustive criteria" defined by the audited service within the 2024 SRA documentation that was used to assess whether the factors referred to in Article 34.2 influence the systemic risks identified across each service. Inspected the list of criteria, which included consideration of the presence of external risk factors (e.g., intentional manipulation of the service, including inauthentic use or automated exploitation of the service) and internal risk factors (e.g., design of recommender and content moderation systems, applicable terms and conditions, etc.), which informs, in part, the audited service's probability and preparedness rationales for each risk statement. Per inspection of the 2024 SRA documentation, determined that the audited service appropriately identified the factors referred to in Article 34.2 and that the rationale for each risk associated with the audited service that was documented within the risk assessment as well as in certain instances, obtained through additional inquiries performed with management, generally demonstrated how these factors could impact the service.

Additionally, per inspection of the rationale documented within the risk assessment, determined that the audited service appropriately identified and assessed how the risks identified for the audited service are influenced by intentional manipulation of their service, including by inauthentic use or automated exploitation of the of the service as well as amplification and potentially rapid and wide dissemination of illegal content and of information that is incompatible with their terms and conditions, in accordance with Recital 84.

With respect to regional or linguistic aspects of the services, inspected the assessment results and determined that risk statements were identified for inadequacies related to languages/dialects or markets. Additionally, where relevant, the assessment rationales also include commentary on regional or linguistic aspects of the services as part of the assessment performed over the risk factors that influence the systemic risks. As such, determined that the 2024 SRA took into account specific regional or linguistic aspects, including where specific to a Member State.

Inquired with management and for a sample content moderation system, sampled in accordance with the sampling approach described in Appendix 2, inspected system documentation, dashboards and reports and ascertained that the system performance and quality was monitored for the duration of the DSA Examination Period, and there were no significant changes in model performance based on pre-defined thresholds. Inspected system and process documentation and determined that a formal process is in place to investigate anomalies and update the model logic, if needed. Inspected change management policies, procedures and documentation and determined that the policies require segregation of duties for approval and implementation of any changes.

Inquired with management throughout the DSA Examination Period and inspected an infrastructure supporting the recommender system architecture which supports recommendations made on all VLOPs and VLOSE and process



documentation related to that recommender system architecture and determined that it was managed using a combination of common system workflows and tools. Inspected the recommender system architecture model documentation and code and determined that the system functionality did not change significantly throughout the DSA Examination Period. Inspected system code and documentation evidence and determined that the user's preference and selection is used as input by the recommender system. Inspected system documentation, dashboards and reports and determined that the system performance and quality was monitored for the duration of the DSA Examination Period, and there were no significant changes in model performance based on pre-defined thresholds.

4. Inspected relevant IT controls, including controls related to change management and logical access, for the relevant systems in the production environment and determined that the controls were in place throughout the DSA Examination Period to address key IT risks.

5. Inquired with management and management noted that no significant changes were made to the policies, processes and/or controls after the walkthrough had been conducted through the end of the DSA Examination Period.

#### **Changes to the audit procedures during the audit:**

None.

#### **Results of procedures performed, how reasonable level of assurance was achieved, and conclusion:**

There were no material deviations identified in the performance of the above procedures, unless denoted below. The results of the audit procedures were deemed sufficient to obtain reasonable assurance.

**Positive with comments** - In our opinion, the audited service complied with this DSA Specified Requirement during the DSA Examination Period, in all material respects.

See below Recommendation on specific measures.

#### **Recommendations on specific measures:**

- (a) Pursuant to Article 34.2, as a recommended enhancement to the risk assessment process, the evidence documented in the SRA should clearly articulate the rationale and provide more detail of how the risk factors in Article 34.2 were evaluated at the risk statement level, to demonstrate the extent to which such factors influence the systemic risks identified.
- (b) Pursuant to Article 34.2, as a recommended enhancement to future off-cycle risk assessments, to ensure the risk assessment is appropriately documented, the off-cycle assessment template should clearly be designed to address the factors referred to in Article 34.2, with, for example, a section allowing for information related to those factors and information about the extent such factors influence the risks.

#### **Recommended timeframe to implement specific measures:**

- (a) 30 September 2024 - 28 August 2025
- (b) 28 August 2025 - 28 February 2026



<b>Obligation:</b>	<b>Audit criteria:</b>	<b>Materiality threshold:</b>
34.3	<p>Throughout the period, in all material aspects:</p> <ol style="list-style-type: none"> <li>1. The provider preserved supporting documents of the risk assessments for at least three years after the performance of risk assessments.</li> <li>2. If requested, supporting documents were communicated to the Commission and to the Digital Services Coordinator of establishment.</li> </ol> <p><b>Note:</b> The audit criteria is supplemented by any additional provisions as outlined in Article 13 of the Delegated Regulation.</p>	<p>If a control was not suitably designed and operated effectively to satisfy the obligation for at least 95% of the DSA Examination Period, and/or if there was an actual or projected error of more than 5% (or other material qualitative variance) during the DSA Examination Period related to the audit criteria.</p>
<p><b>Audit procedures and information relied upon:</b></p> <p>In order to evaluate the audited service's compliance with this DSA Specified Requirement, we evaluated the design and operation of controls and performed substantive procedures, as outlined below:</p> <ol style="list-style-type: none"> <li>1. Conducted a walkthrough and inquired with management to gain an understanding of the process in place to preserve supporting documents of the risk assessments for at least three years after the performance of risk assessments and communicate supporting documentation of the Systemic Risk Assessment (SRA) to the Commission and Digital Services Coordinator (DSC), upon request.</li> <li>2. Assessed the policies, processes, and controls in place to evaluate the audited service's compliance with this DSA Specified Requirement.</li> </ol> <p>Inspected the SRA Playbook and determined that it defined the requirements for preservation of the 2024 SRA's supporting documents, including the report itself, for the regulatory mandated minimum period of three years. Inspected the storage location where all supporting documentation of the 2024 SRA, including the report itself was stored, and determined that the retention policy and user access restrictions for the storage location was appropriate to ensure that the documentation was retained for the regulatory-defined retention period of at least 3 years.</p> <ol style="list-style-type: none"> <li>3. Inquired with management and determined that there were no Requests for Information (RFIs) issued by the Commission for the 2024 SRA's supporting documents or the DSC for the audited service during the DSA Examination Period.</li> <li>4. Inspected the designated storage drive and the supporting documents retained within the drive's folders and determined that the audited service correctly identified the supporting documentation that should be preserved with respect to the 2024 SRA.</li> <li>5. Inquired with management and management noted that no significant changes were made to the policies, processes and/or controls after the walkthrough had been conducted through the end of the DSA Examination Period.</li> </ol> <p><b>Changes to the audit procedures during the audit:</b></p>		



None.

**Results of procedures performed, how reasonable level of assurance was achieved, and conclusion:**

There were no material deviations identified in the performance of the above procedures, unless denoted below. The results of the audit procedures were deemed sufficient to obtain reasonable assurance.

**Positive** - In our opinion, the audited service complied with this DSA Specified Requirement during the DSA Examination Period, in all material respects.

**Recommendations on specific measures:**

Not applicable.

**Recommended timeframe to implement specific measures:**

Not applicable.

<b>Obligation:</b>	<b>Audit criteria:</b>	<b>Materiality threshold:</b>
35.1	<p>Throughout the period, in all material aspects:</p> <ol style="list-style-type: none"> <li>1. Reasonable, proportionate and effective mitigation measures were put in place tailored to the specific systemic risks identified pursuant to Article 34.</li> <li>2. The provider considered the impact of the mitigation measures on the fundamental rights of the recipients of the service.</li> <li>3. The risk assessment included an assessment whether the risk mitigation measures in Article 35.1, points (a) to (k) were applicable to the audited service.</li> </ol> <p><b>Note:</b> The audit criteria is supplemented by any additional provisions as outlined in Article 14 of the Delegated Regulation.</p> <p><b>The following are certain operational benchmark(s) defined by the audited service:</b></p> <p>“reasonable, proportionate, effective measures”: mitigation measures / action plans put in place to address systemic risks identified during the risk assessment in areas of heightened residual risk (can be tied to objectives and key results (OKRs), Launches, Programs, etc.) and – combined with the suite of other relevant mitigations – have the effect of lessening (or keeping stable) levels of systemic risk while being commensurate to the severity and probability, recognizing that external factors are dynamic and may change.</p>	<p>If a control was not suitably designed and operated effectively to satisfy the obligation for at least 95% of the DSA Examination Period, and/or if there was an actual or projected error of more than 5% (or other material qualitative variance) during the DSA Examination Period related to the audit criteria.</p>





### Audit procedures and information relied upon:

In order to evaluate the audited service's compliance with this DSA Specified Requirement, we evaluated the design and operation of controls and performed substantive procedures, as outlined below:

1. Conducted a walkthrough and inquired with management to gain an understanding of the policies and processes in place to ensure reasonable, proportionate and effective mitigation measures are put in place tailored to the specific systemic risks identified pursuant to Article 34. In addition, obtained an understanding of the impact of such measures on the fundamental rights of the recipients of the service and whether the audited service determined the applicability of the risk mitigation measures in Article 35.1, points (a) to (k).
2. Assessed the design of the policies, processes, and controls in place, and determined that the policies, processes, and suite of controls in place were appropriately designed and were operating effectively. Inspected the SRA Playbook and supporting slide decks that describe the risk mitigation monitoring process and determined that it specified the process by which the applicable VLOPs and the VLOSE respond to the risk assessment results by putting in place reasonable, proportionate, and effective mitigation measures.

Inspected a sample of email communications between the central 2024 SRA team and product teams, sampled in accordance with the sampling approach described in Appendix 2, and determined that periodic communication existed to monitor accountability. In addition, inspected evidence of trackers maintained and email communications between internal teams and determined that the central 2024 SRA team periodically communicated with the relevant stakeholders of the audited service to monitor status of implementation of additional mitigation measures put in place pursuant to the SRA Playbook in accordance with Article 35. Inspected evidence of the audited service's internal validation documentation performed by an independent team that is not involved in the execution of the 2024 SRA, and determined that each enhanced mitigation that had completed validation per the Enhanced Mitigations Tracker during the DSA Examination Period had been validated by this team to indicate that it had been successfully launched, as denoted by supporting documentation retained as evidence of the implementation of the mitigation measure and sign-offs by the independent team within the documentation retained.

For a sample of enhanced mitigation measures for which the audited service had completed the implementation and evaluation, sampled in accordance with the sampling approach described in Appendix 2, inspected evidence of the audited service's validation documentation to understand how these mitigation measures were designed and implemented. Further inspected supporting documentation for each sampled mitigation measure such as, narratives describing product requirement documentation, launch approvals and implementation metrics and determined that the independent team had appropriately validated the successful launch of the mitigation measure.

3. Inspected the audited service's 2024 SRA documentation, internal trackers, and the 'Report of Systemic Risk Assessments' issued by the audited service and determined that Article 35 mitigation measures were identified for each systemic risk where the residual risk scores met the threshold for enhancements as explained in the audited service's SRA Playbook. We determined that the identification of risk mitigation measures for the systemic risks was carried out in a diligent manner.

Additionally, through inspection of the descriptions and action plan for each Article 35 mitigation measure mapped to the systemic risks, determined that risk mitigation measures for each of the systemic risks were identified, as well as the rationale provided by the audited service for mitigation measures in Article 35.1 points (a) to (k) that were not implemented following the 2024 SRA, and that each enhanced mitigation measure to be implemented was assessed for its applicability to the risk mitigation measures in Article 35.1, points (a) to (k) and to the applicable audited service.

Inspected the audited service's 2024 SRA conducted for the audited service, and determined that a holistic approach to evaluating mitigations was performed to assess whether the mitigations put in place by the audited service respond





collectively to all risks in a reasonable, proportionate, and effective manner, by assessing how both existing mitigations and enhanced mitigations put in place respond to the applicable risks. Additionally, inspected the mitigation measures documented within the 2024 SRA and determined that the 2024 SRA explicitly referenced proportionality principles, such as prioritizing visibility restrictions over removals, enabling appeals mechanisms, and tailoring enforcement to minimize unnecessary impacts on users' rights, thereby indicating that there was particular consideration of the risks concerning the exercise of fundamental rights.

Inspected the audited service's 2024 SRA and determined that the audited service reevaluated the risk statement preparedness score before and after the closure of each enhanced mitigation put in place. Assessed, comparatively, how the risks were addressed before and after the specific risk mitigation measures were put in place through inclusion of documented rationale of whether and how the preparedness scores were influenced by the enhanced mitigation.

To assess whether the mitigation measures were appropriately designed and executed, inspected the audited service's 2024 SRA conducted for the audited service and determined that the assessment of each risk statement's concluding residual risk score reflected an assessment of the design and execution of mitigations (both existing and enhanced) by considering how the mitigation is designed and what risk(s) it is designed to address and how well the design (if operating as intended) mitigates that specific risk statement as reflected in the preparedness scores.

Inspected the compliance monitoring plan and determined the ICF had a process to monitor the compliance of the audited service with its obligations under the DSA through performing internal controls validation and validation of completed remediation. To corroborate the aforementioned procedures performed by the ICF, inquired with the head compliance officer and confirmed that the ICF actively monitored the audited service's compliance with its obligations under the DSA throughout the DSA Examination Period. Additionally, inspected the agendas and excerpts of meeting minutes of quarterly board meetings and ad hoc meetings, and determined the compliance monitoring plan had been reviewed and approved by the management body, and ICF provided status updates on the control validation process to demonstrate their monitoring of the compliance of the audited service with its obligation.

To assess the involvement of the management body of the audited provider in decisions related to risk management pursuant to Article 41.6 and 41.7, inspected meeting agendas and excerpts of meeting minutes of quarterly board meetings and ad hoc meetings and determined that the results of the independent 2024 SRA assessment performed by the ICF were presented to the management body and 2024 SRA team.

Inspected meeting agendas and excerpts of the quarterly board meeting minutes and ad hoc meetings and determined the management body devoted sufficient time to the consideration of the measures related to risk management, maintained active involvement in the decisions related to risk management, and ensured that adequate resources were allocated to the management of the risks identified in accordance with Article 34 as part of the ICF's independent 2024 SRA assessment. Evaluated the sufficiency of time devoted by the management body considering the ad hoc meetings scheduled between the compliance function and management body throughout the DSA Examination Period, in addition to their quarterly meetings. To corroborate the aforementioned procedures performed by the management body, inquired with the management board and confirmed that the management body devoted sufficient time during the scheduled board meetings to DSA risk management decisions and processes and was actively involved in the decisions related to risk management.

Inspected the 'Report of Systemic Risk Assessments' issued by the audited service, and its underlying documentation, to determine adequate comprehensiveness of actions taken and adequacy of information in support of the assessment carried out pursuant to this article. The inspection included, but was not limited to, the following elements:



- Reviewed the reports on risk assessment and risk mitigation for the DSA Examination Period prepared by the audited service along with the supporting documents.
  - Evaluated information submitted by the audited service pursuant to Article 5 of the Delegated Regulation on the performance of audits, verifying its relevance and accuracy in the context of the risk assessment.
  - Analyzed all relevant transparency reports of the audited provider referred to in Article 15.1 to assess the audited service's disclosure and transparency regarding the risk assessment.
  - Assessed other relevant evidence (including test results, documentation, and statements made in response to written or oral questions) provided by the audited service to ensure a thorough understanding of the risk assessment.
  - Assessed reports referred to in Article 35.2 of Regulation (EU) 2022/2065 and guidance from the Commission, including guidelines issued pursuant to Article 35.3 of that Regulation and any other relevant guidance issued by the Commission with respect to the application of Regulation (EU) 2022/2065 to confirm inclusion in the risk assessment.
- Inquired with management and determined that no other risk assessment reports were considered relevant in support of the assessment carried out pursuant to this article.
4. Inquired with management and management noted that no significant changes were made to the policies, processes and/or controls after the walkthrough had been conducted through the end of the DSA Examination Period.

#### **Changes to the audit procedures during the audit:**

None.

#### **Results of procedures performed, how reasonable level of assurance was achieved, and conclusion:**

There were no material deviations identified in the performance of the above procedures, unless denoted below. The results of the audit procedures were deemed sufficient to obtain reasonable assurance.

**Positive with comments** - In our opinion, the audited service complied with this DSA Specified Requirement during the DSA Examination Period, in all material respects.

See below Recommendation on specific measures.

#### **Recommendations on specific measures:**

Pursuant to Article 35.1, as an enhancement to the risk assessment and mitigation process, the audited service should enhance documentation of the relevant considerations that support its scoring rationale and include sufficient information to support reperformance of risk rating for relevant risk statements as part of audit testing.

The audited provider should also consider improvement in tracking timelines (target and actual) for the implementation, validation and closure of mitigations within the enhanced mitigation tracker.

#### **Recommended timeframe to implement specific measures:**

28 August 2025 - 28 February 2026



In addition, the audited provider should also consider enhancing their 'enhanced risk mitigation trackers' to facilitate more detailed tracking of the status of mitigations, and ensure the risk mitigation trackers comprehensively reflect progress, including issues encountered, deprecated mitigations and consolidated mitigations.	
--	--

Obligation:	Audit criteria:	Materiality threshold:
36.1	<p>Throughout the period, in all material aspects:</p> <p>1. Upon a decision adopted by the Commission in respect of a crisis, the provider took one or more of the following actions (as required by the Commission):</p> <ul style="list-style-type: none"><li>- assessed whether, and if so to what extent, the functioning and use of their service significantly contribute to a serious threat as referred to in Article 36.2 or are likely to do so,</li><li>- identified and applied specific, effective and proportionate measures to prevent, eliminate or limit any such contribution to the serious threat, and</li><li>- reported to the Commission by a certain date or at regular intervals as specified in the decision the precise content, implementation and qualitative and quantitative impact of the specific measures taken and on any other issue related to those assessments or those measures, as specified in the decision.</li></ul> <p>2. In identifying and applying specific, effective and proportionate measures, the provider took due account of the gravity of the serious threat; the urgency of the measures and of the actual or potential implications for the rights and legitimate interests of all parties concerned, including the possible failure of the measures to respect the fundamental rights enshrined in the Charter.</p> <p><b>Note:</b> The audit criteria is supplemented by any additional provisions as outlined in Article 15 of the Delegated Regulation.</p>	<p>If a control was not suitably designed and operated effectively to satisfy the obligation for at least 95% of the DSA Examination Period, and/or if there was an actual or projected error of more than 5% (or other material qualitative variance) during the DSA Examination Period related to the audit criteria.</p>

<p><b>Audit procedures and information relied upon:</b></p> <p>In order to evaluate the audited service’s compliance with this DSA Specified Requirement, we performed substantive procedures, although controls existed<sub>1</sub> as outlined below:</p> <p>1. Conducted a walkthrough and inquired with management and determined there were no occurrences of a serious threat or crisis declared by the Commission to the audited provider during the period 1 June 2024 through 31 May 2025.</p>
---



2. Inquired with management to gain an understanding of the procedures and policies in place for when a crisis is declared by the Commission, and per inspection of the policy documentation determined it included guidance to assess whether, and if so to what extent, the functioning and use of their service significantly contribute to the serious threat or are likely to do so; identify relevant systems involved in the functioning or use of the service(s) that significantly contributes to the serious threat; identify and apply specific, effective and proportionate measures to prevent, eliminate or limit any such contribution to the serious threat; identify the parties concerned by the measures, and assess the actual or potential impact of the measures on those parties' fundamental rights and legitimate interests; and report to the Commission by a certain date or at regular intervals as specified in the Commission's decision.

3. Assessed that the policies and processes were appropriate to comply with the DSA Specified Requirements, if an occurrence of a Commission-declared crisis were to take place. Furthermore, determined through inspection that the policy was effective for the duration of the DSA Examination Period.

4. Inquired with management and management noted that no significant changes were made to the policies, processes and/or controls after the walkthrough had been conducted through the end of the DSA Examination Period.

**Changes to the audit procedures during the audit:**

None.

**Results of procedures performed, how reasonable level of assurance was achieved, and conclusion:**

There were no material deviations identified in the performance of the above procedures, unless denoted below. The results of the audit procedures were deemed sufficient to obtain reasonable assurance.

**Positive** - In our opinion, the audited service complied with this DSA Specified Requirement during the DSA Examination Period, in all material respects.

**Recommendations on specific measures:**

Not applicable.

**Recommended timeframe to implement specific measures:**

Not applicable.

Obligation:	Audit criteria:	Materiality threshold:
37.1	<p>The provider was subject, at their own expense, to an independent audit for the prior year to assess compliance with the obligations set out in Chapter III and any commitments undertaken pursuant to the codes of conduct referred to in Articles 45 and 46 and crisis protocols referred to in Article 48.</p> <p><b>Note:</b> The audit criteria are supplemented by the additional provisions as outlined in Article 16 of the Delegated Regulation.</p>	<p>If a control was not suitably designed and operated effectively to satisfy the obligation for at least 95% of the DSA Examination Period, and/or if there was an actual or projected error of more than 5% (or other material qualitative variance) during the DSA Examination Period related to the audit criteria.</p>
<b>Audit procedures and information relied upon:</b>		



In order to evaluate the audited service's compliance with this DSA Specified Requirement, we performed substantive procedures, although controls existed, as outlined below:

1. Inquired with management to gain an understanding of their process to obtain an annual independent audit in the prior year.
2. Inspected the audited provider and auditing organization's executed Statement of Work from the prior year audit and validated that the audit was performed at the audited provider's expense. To determine whether the audit assessed compliance with the required obligations, inspected the prior year's issued audit report and identified that the scope of the audit included all applicable obligations set out in Chapter III of Regulation (EU) 2022/2065. To determine whether the audit assessed compliance with the required commitments undertaken pursuant to codes of conduct, inspected the prior year's issued audit report and Statement of Work and determined that there were no applicable commitments included within the scope of the audit, as such requirement did not exist during the relevant period.
3. Inquired with management noting that no significant changes were made to the policies, processes and controls through the end of the DSA Examination Period.

**Changes to the audit procedures during the audit:**

None.

**Results of procedures performed, how reasonable level of assurance was achieved, and conclusion:**

There were no material deviations identified in the performance of the above procedures, unless denoted below. The results of the audit procedures were deemed sufficient to obtain reasonable assurance.

**Positive** - In our opinion, the audited service complied with this DSA Specified Requirement during the DSA Examination Period, in all material respects.

**Recommendations on specific measures:**

Not applicable.

**Recommended timeframe to implement specific measures:**

Not applicable.

Obligation:	Audit criteria:	Materiality threshold:
37.2	<p>Throughout the period, in all material aspects:</p> <p>As part of the audit, the provider:</p> <ul style="list-style-type: none"> <li>- gave the auditors the necessary cooperation and assistance to enable them to conduct the audit in an effective, efficient and timely manner, including by giving</li> <li>- access to all relevant data and premises and by answering oral or written questions timely, and</li> <li>- refrained from hampering, unduly influencing or undermining the performance of the audit.</li> </ul>	<p>If a control was not suitably designed and operated effectively to satisfy the obligation for at least 95% of the DSA Examination Period, and/or if there was an actual or projected error of more than 5% (or other material qualitative variance) during the DSA Examination Period related to the audit criteria.</p>



	<p><b>Note:</b> The audit criteria are supplemented by the additional provisions as outlined in Article 16 of the Delegated Regulation.</p>	
<p><b>Audit procedures and information relied upon:</b></p> <p>In order to evaluate the audited service's compliance with this DSA Specified Requirement, we performed substantive procedures, although controls existed, as outlined below:</p> <p>1. Inquired of relevant team members who interacted with audited provider personnel, and validated that there have not been any material situations where the audited service:</p> <ul style="list-style-type: none"> <li>- did not afford the auditing organization cooperation and assistance necessary to enable the auditing organization to conduct the current year audit in an effective, efficient and timely manner,</li> <li>- refused to give the auditing organization access to all relevant data and premises, or did not answer oral or written questions, and</li> <li>- hampered, unduly influenced, or undermined the performance of the current year audit.</li> </ul> <p><b>Changes to the audit procedures during the audit:</b></p> <p>None.</p> <p><b>Results of procedures performed, how reasonable level of assurance was achieved, and conclusion:</b></p> <p>There were no material deviations identified in the performance of the above procedures, unless denoted below. The results of the audit procedures were deemed sufficient to obtain reasonable assurance.</p> <p><b>Positive</b> - In our opinion, the audited service complied with this DSA Specified Requirement during the DSA Examination Period, in all material respects.</p>		
<p><b>Recommendations on specific measures:</b></p> <p>Not applicable.</p>	<p><b>Recommended timeframe to implement specific measures:</b></p> <p>Not applicable.</p>	



<b>Obligation:</b>	<b>Audit criteria:</b>	<b>Materiality threshold:</b>
37.3	<p>In relation to the independent audit performed for the prior year, in all material aspects, the provider ensured the audit was performed by organizations which:</p> <ul style="list-style-type: none"> <li>- are independent from and do not have any conflicts of interest with the provider and any legal person connected to that provider. Specifically, these organizations:</li> <li>- have not provided non-audit services related to the matters audited to the provider and to any legal person connected to that provider in the 12 months' period before the beginning of the audit and have committed to not providing them with such services in the 12 months' period after the completion of the audit.</li> <li>- have not provided auditing services pursuant to Article 37 to the provider and any legal person connected to that provider during a period longer than 10 consecutive years.</li> <li>- are not performing the audit in return for fees which are contingent on the result of the audit.</li> <li>- have proven expertise in the area of risk management, technical competence and capabilities.</li> <li>- have proven objectivity and professional ethics, based in particular on adherence to codes of practice or appropriate standards.</li> </ul> <p><b>Note:</b> The audit criteria are supplemented by the additional provisions as outlined in Article 16 of the Delegated Regulation.</p>	<p>If a control was not suitably designed and operated effectively to satisfy the obligation for at least 95% of the DSA Examination Period, and/or if there was an actual or projected error of more than 5% (or other material qualitative variance) during the DSA Examination Period related to the audit criteria.</p>
<p><b>Audit procedures and information relied upon:</b></p> <p>In order to evaluate the audited service's compliance with this DSA Specified Requirement, we performed substantive procedures, although controls existed, as outlined below:</p> <ol style="list-style-type: none"> <li>1. Inquired with management to gain an understanding of their process for ensuring that the auditing organization met the requirement specified within Article 37.3. Determined that management conducted an assessment of the auditing organization's qualifications, focusing on their technical skills and understanding of management's systems. As part of management's evaluation, management also relied on representations made by the auditing organization about their expertise in risk management, technical competencies, and capabilities, independence, and adherence to appropriate professional standards.</li> <li>2. Inspected the audited service's independent auditor assessment and independent audit questionnaire from the prior year and ensured that the assessment took into consideration the requirement specified within Article 37.3.</li> </ol> <p>Inspected the audited provider and auditing organization's executed Statement of Work from the prior year and determined that the audit was not performed in return for fees contingent on the outcome of the audit, the auditing organization represented that they met the relevant independent requirements related to the audited service pursuant</p>		



to Article 37.3, and the audit was performed in accordance with relevant professional standards with requirements related to objectivity and professional ethics.

3. Inquired with management noting that no significant changes were made to the policies, processes and controls through the end of the DSA Examination Period.

**Changes to the audit procedures during the audit:**

None.

**Results of procedures performed, how reasonable level of assurance was achieved, and conclusion:**

There were no material deviations identified in the performance of the above procedures, unless denoted below. The results of the audit procedures were deemed sufficient to obtain reasonable assurance.

**Positive** - In our opinion, the audited service complied with this DSA Specified Requirement during the DSA Examination Period, in all material respects.

**Recommendations on specific measures:**

Not applicable.

**Recommended timeframe to implement specific measures:**

Not applicable.

<b>Obligation:</b>	<b>Audit criteria:</b>	<b>Materiality threshold:</b>
37.4	<p>In relation to the independent audit performed for the prior year, in all material aspects, the provider ensured that the auditing organizations established an audit report for each audit that was substantiated, in writing, and included the components specified in Article 37.4.</p> <p><b>Note:</b> The audit criteria are supplemented by the additional provisions as outlined in Article 16 of the Delegated Regulation.</p>	<p>If a control was not suitably designed and operated effectively to satisfy the obligation for at least 95% of the DSA Examination Period, and/or if there was an actual or projected error of more than 5% (or other material qualitative variance) during the DSA Examination Period related to the audit criteria.</p>
<b>Audit procedures and information relied upon:</b>		
<p>In order to evaluate the audited service's compliance with this DSA Specified Requirement, we performed substantive procedures, although controls existed, as outlined below:</p>		
<p>1. Inquired with management to gain an understanding of their process for ensuring that the audit report included the components specified in Article 37.4.</p>		
<p>2. Inspected the prior year audit report and determined that the report included the required information specified within Article 37.4.</p>		



**Changes to the audit procedures during the audit:**

None.

**Results of procedures performed, how reasonable level of assurance was achieved, and conclusion:**

There were no material deviations identified in the performance of the above procedures, unless denoted below. The results of the audit procedures were deemed sufficient to obtain reasonable assurance.

**Positive** - In our opinion, the audited service complied with this DSA Specified Requirement during the DSA Examination Period, in all material respects.

**Recommendations on specific measures:**

Not applicable.

**Recommended timeframe to implement specific measures:**

Not applicable.

<b>Obligation:</b>	<b>Audit criteria:</b>	<b>Materiality threshold:</b>
37.5	<p>In relation to the independent audit performed for the prior year, in all material aspects, where the auditing organization was unable to assess certain specific elements or express an audit opinion based on its investigations, the audit report included an explanation of the circumstances and the reasons why those elements could not be audited.</p> <p><b>Note:</b> The audit criteria are supplemented by the additional provisions as outlined in Article 16 of the Delegated Regulation.</p>	<p>If a control was not suitably designed and operated effectively to satisfy the obligation for at least 95% of the DSA Examination Period, and/or if there was an actual or projected error of more than 5% (or other material qualitative variance) during the DSA Examination Period related to the audit criteria.</p>

**Audit procedures and information relied upon:**

In order to evaluate the audited service's compliance with this DSA Specified Requirement, we performed substantive procedures, although controls existed, as outlined below:

1. Inquired with management to gain an understanding of their process for ensuring that the audit report included an explanation of the circumstances and reasons why certain elements could not be audited, where applicable.
2. Inspected the prior year audit report to identify specific elements that could not be audited or for which an audit opinion could not be expressed and determined that the report includes an explanation of the circumstances and the reasons why those elements could not be audited.

**Changes to the audit procedures during the audit:**

None.


**Results of procedures performed, how reasonable level of assurance was achieved, and conclusion:**

There were no material deviations identified in the performance of the above procedures, unless denoted below. The results of the audit procedures were deemed sufficient to obtain reasonable assurance.

**Positive** - In our opinion, the audited service complied with this DSA Specified Requirement during the DSA Examination Period, in all material respects.

**Recommendations on specific measures:**

Not applicable.

**Recommended timeframe to implement specific measures:**

Not applicable.

<b>Obligation:</b>	<b>Audit criteria:</b>	<b>Materiality threshold:</b>
37.6	<p>In relation to the independent audit performed for the prior year, in all material aspects, where the audit report contained conclusions that were not 'positive', the provider:</p> <ul style="list-style-type: none"> <li>- took due account of the operational recommendations addressed to them with a view to taking the necessary measures to implement them and, within one month of receiving these operational recommendations, adopted an audit implementation report setting out those measures.</li> <li>- justified in the audit implementation report any reasons for not implementing the operational recommendations and set out any alternative measures taken to address any instances of identified non-compliance.</li> </ul> <p><b>Note:</b> The audit criteria are supplemented by the additional provisions as outlined in Article 16 of the Delegated Regulation.</p>	<p>If a control was not suitably designed and operated effectively to satisfy the obligation for at least 95% of the DSA Examination Period, and/or if there was an actual or projected error of more than 5% (or other material qualitative variance) during the DSA Examination Period related to the audit criteria.</p>

**Audit procedures and information relied upon:**

In order to evaluate the audited service's compliance with this DSA Specified Requirement, we performed substantive procedures, although controls existed, as outlined below:

1. Inquired with management to gain an understanding of their process to address the operational recommendations provided by the auditing organization in the prior year audit report. Management noted that they had a formal process for assessing recommendations and implementing select recommendations through a variety of means including enhancing process and controls and reevaluating benchmarks. For recommendations not implemented, the audited service justified reasons for not implementing the recommendation and listed alternative measures taken in the audit implementation report.
2. Compared the prior year audit implementation report with the prior year audit report and determined that the audited provider addressed the operational recommendations for all conclusions that were not "positive" and, for any instances



<p>where the audited provider did not implement the operational recommendations, inspected the report to ensure that the audited service provided reasons for not implementing the operational recommendations and stated alternative measures taken.</p> <p>Inspected e-mail correspondence from the audited provider to the Digital Services Coordinator on 27 October 2024 transmitting the implementation report. The prior year audit report was issued on 27 September 2024, therefore the implementation report was adopted within one month of receiving the operational recommendations from the auditing organization.</p> <p>3. Inquired with management and management noted that no significant changes were made to the policies, processes and controls through the end of the DSA Examination Period.</p> <p><b>Changes to the audit procedures during the audit:</b></p> <p>None.</p> <p><b>Results of procedures performed, how reasonable level of assurance was achieved, and conclusion:</b></p> <p>There were no material deviations identified in the performance of the above procedures, unless denoted below. The results of the audit procedures were deemed sufficient to obtain reasonable assurance.</p> <p><b>Positive</b> - In our opinion, the audited service complied with this DSA Specified Requirement during the DSA Examination Period, in all material respects.</p>		
<p><b>Recommendations on specific measures:</b></p> <p>Not applicable.</p>		<p><b>Recommended timeframe to implement specific measures:</b></p> <p>Not applicable.</p>
<p><b>Obligation:</b></p> <p>38</p>	<p><b>Audit criteria:</b></p> <p>Throughout the period, in all material aspects:</p> <p>Providers of very large online platforms and of very large online search engines that use recommender systems provided at least one option for each of their recommender systems which was not based on profiling as defined in Article 4.4, or Regulation (EU) 2016/679.</p>	<p><b>Materiality threshold:</b></p> <p>If a control was not suitably designed and operated effectively to satisfy the obligation for at least 95% of the DSA Examination Period, and/or if there was an actual or projected error of more than 5% (or other material qualitative variance) during the DSA Examination Period related to the audit criteria.</p>
<p><b>Audit procedures and information relied upon:</b></p> <p>In order to evaluate the audited service’s compliance with this DSA Specified Requirement, we evaluated the design and operation of controls and performed substantive procedures, as outlined below:</p>		



1. Conducted a walkthrough and inquired with management to gain an understanding of the mechanisms recipients of the service (users) can use to disable profiling-based recommendations by managing Web & App Activity, Timeline, and additional settings such as deleting past activity and deleting Location History. The mechanism recipients of the service can use to disable profiling-based recommendations for advertisements shown on the audited service is by managing settings related to personalized advertisements.
2. Inspected the audited service's underlying code during the DSA Examination Period and determined that its functionality allows recipients of the service the option to disable profiling-based recommendations.
3. Inspected the Transparency Centre and Help Centre and determined an option to disable profiling was provided. Performed user journey testing using the options to turn the profiling-based recommendations off. Inspected the results of the recommender system before and after disabling profiling-based system settings and determined that the recommendations were not based on profiling when the profiling-based system settings were off.
4. Inquired with management throughout the DSA Examination Period, and inspected an infrastructure supporting the recommender system architecture, which supports recommendations made on all VLOPs and VLOSE and process documentation related to that recommender system architecture and determined that it was managed using a combination of common system workflows and tools. Inspected the recommender system architecture model documentation and code and determined that the system functionality did not change significantly throughout the DSA Examination Period. Inspected system code and documentation evidence and determined that the user's preference and selection is used as input by the recommender system. Inspected system documentation, dashboards and reports and determined that the system performance and quality was monitored for the duration of the DSA Examination Period, and there were no significant changes in model performance based on pre-defined thresholds.
5. Inspected the systemic risk assessment performed for the audited service pursuant to Article 34 and noted that the risk statements identified included topics covered under this sub article. In addition, the audited service identified mitigation measures related to the risk factors which we assessed under Article 34.
6. Inspected relevant IT controls, including controls related to change management and logical access, for the relevant systems in the production environment and determined that the controls were in place throughout the DSA Examination Period to address key IT risks.
7. Inquired with management and management noted that no significant changes were made to the policies, processes and/or controls after the walkthrough had been conducted through the end of the DSA Examination Period.

**Changes to the audit procedures during the audit:**

None.

**Results of procedures performed, how reasonable level of assurance was achieved, and conclusion:**

There were no material deviations identified in the performance of the above procedures, unless denoted below. The results of the audit procedures were deemed sufficient to obtain reasonable assurance.

**Positive** - In our opinion, the audited service complied with this DSA Specified Requirement during the DSA Examination Period, in all material respects.



<b>Recommendations on specific measures:</b>  Not applicable.	<b>Recommended timeframe to implement specific measures:</b>  Not applicable.
---	---

Obligation:	Audit criteria:	Materiality threshold:
39.1	<p>Throughout the period, in all material aspects:</p> <ol style="list-style-type: none"> <li>The provider, which presents advertisements on their online interfaces, compiled and made available an online repository which:               <ul style="list-style-type: none"> <li>- was publicly available on their online interface,</li> <li>- contained information described in Article 39.2,</li> <li>- had a search function that allowed multicriteria queries,</li> <li>- made information available using application programming interfaces, and</li> <li>- did not contain any personal data of the recipients of the service to whom the advertisement was or could have been presented.</li> </ul> </li> <li>The provider ensured that the advertisement information in the repository was available for the entire period that the advertisement was presented and one year after the advertisement was last shown and made reasonable efforts to ensure that the advertisement information in the repository was accurate and complete.</li> </ol> <p><b>The following are certain operational benchmark(s) defined by the audited service:</b></p> <p>"for the entire period during which they present an advertisement": provide the relevant data for the period of time for which the advertisement was presented on the service.</p>	<p>If a control was not suitably designed and operated effectively to satisfy the obligation for at least 95% of the DSA Examination Period, and/or if there was an actual or projected error of more than 5% (or other material qualitative variance) during the DSA Examination Period related to the audit criteria.</p>

#### Audit procedures and information relied upon:

In order to evaluate the audited service's compliance with this DSA Specified Requirement, we evaluated the design and operation of controls and performed substantive procedures, as outlined below:

- Conducted a walkthrough and inquired with management to gain an understanding of how the audited service made available an online repository which met the DSA Specified Requirement set forth within this sub article. The Ads Transparency Center (ATC), located at [adstransparency.google.com](https://adstransparency.google.com), allows recipients of the service to select and apply multi criteria filter and search capabilities, and made publicly available the information referred to in Article 39.2 through a user interface (UI) and also through application programming interfaces (API). The recipient of the service is



able to see the following information for each advertisement: advertisement content (creative), subject matter of the advertisement, advertiser name, ad funded by (when applicable), date range in which the advertisement was presented, information on particular groups targeted for inclusion or exclusion, and total number of recipients reached.

2. Assessed the processes and controls in place and determined that the suite of controls were appropriately designed and operating as intended. Inspected system configurations defined within the production code base and determined that the ATC has a search function configured to allow recipients of the service to select and apply multi-criteria filters to search for advertisement information. Inspected the ATC UI that is publicly available and independently applied filters to search for an advertisement using the search functionality available. Inspected the search results presented within the ATC user interface and determined that advertisements contained information described in Article 39.2.

3. Inspected system configurations defined within the production code base and determined that underlying jobs within the ATC were designed to check the last shown date for an advertisement when a recipient of the service searches for an advertisement and pulls the required information about the advertisement from the ATC storage systems into the ATC UI. Further determined that jobs within the ATC were configured to retrieve and display advertisement's information for up to one year after the advertisement's last impressed date. Selected a sample advertisement, sampled in accordance with the sampling approach described in Appendix 2, and validated that it was available for the entire period that the advertisement was presented and one year after the advertisement was last shown. Further, for the above sample selected, inspected evidence of the job logs for the search executed and determined that the jobs within the ATC ran successfully to check the last shown date for an advertisement when a recipient of the service accesses the ATC, to determine the need to continue including the advertisement and its related information in ATC storage systems.

4. Inspected system configurations defined within the production code base and determined that the data monitoring tool was configured to check for success of data inflows from the central Ads Safety Platform (ASP) into the ATC databases, and that production alerts were configured to be raised to the on-call engineers in the event of a failed process. Inspected a sample successful data inflow from the central ASP into the ATC database during the DSA Examination Period, sampled in accordance with the sampling approach described in Appendix 2 and determined that the log of the dataflow was accurately captured by the data monitoring tool. Selected a sample of failed data inflows, sampled in accordance with the sampling approach described in Appendix 2, from the central ASP into the ATC database during the DSA Examination Period. For each sample, inspected the alerts raised to the on-call engineers and determined the alerts were appropriately investigated and resolved.

5. Inspected the ATC UI and determined that advertisement information was made available using application programming interfaces, and contained information described in Article 39.2. Inspected the ATC UI and the information available through the API and determined that the interface does not contain any personal data of the recipients of the service to whom the advertisement was or could have been presented.

6. Inspected relevant IT controls, including controls related to change management and logical access, for the relevant systems in the production environment and determined that the controls were in place throughout the DSA Examination Period to address the key IT risks.

7. Inquired with management and management noted that no significant changes were made to the policies, processes and/or controls after the walkthrough had been conducted through the end of the DSA Examination Period.

#### **Changes to the audit procedures during the audit:**

None.


**Results of procedures performed, how reasonable level of assurance was achieved, and conclusion:**

There were no material deviations identified in the performance of the above procedures, unless denoted below. The results of the audit procedures were deemed sufficient to obtain reasonable assurance.

**Positive** - In our opinion, the audited service complied with this DSA Specified Requirement during the DSA Examination Period, in all material respects.

**Recommendations on specific measures:**

Not applicable.

**Recommended timeframe to implement specific measures:**

Not applicable.

Obligation:	Audit criteria:	Materiality threshold:
39.2	<p>Throughout the period, in all material aspects:</p> <p>The provider's online repository included the following information for each advertisement:</p> <ul style="list-style-type: none"> <li>(a) the content of the advertisement, including the name of the product, service or brand and the subject matter;</li> <li>(b) the natural or legal person on whose behalf the advertisement is presented;</li> <li>(c) the natural or legal person who paid for the advertisement, if that person is different from the person referred to in the point above;</li> <li>(d) the period during which the advertisement was presented</li> <li>(e) the particular groups of recipients the advertisement was intended to be presented to, and where applicable the main parameters used to exclude such groups;</li> <li>(f) the commercial communications presented on the platform as declared by the recipient of the service;</li> <li>(g) the total number of recipients the advertisement reached, and if applicable, the aggregate numbers broken down by Member States for the group or groups of targeted recipients.</li> </ul> <p><b>The following are certain operational benchmark(s) defined by the audited service:</b></p>	<p>If a control was not suitably designed and operated effectively to satisfy the obligation for at least 95% of the DSA Examination Period, and/or if there was an actual or projected error of more than 5% (or other material qualitative variance) during the DSA Examination Period related to the audit criteria.</p>



	<p>"the natural or legal person who paid for the advertisement if different from the natural or legal person referred to in point (b)": the audited service obtains confirmation that the end-advertiser (i.e., the person on whose behalf the advertisement is presented) is the same as the person paying for the advertisement. This is because in all material respects, the end-advertiser is the person paying for the advertisement, and in situations where an end-advertiser is paying an advertising agency to place an advertisement, regardless of an agency intermediary, the end-advertiser is still the party paying for the advertisement since the advertising agency is being reimbursed by the end-advertiser.</p> <p>"the total number of recipients of the service reached": a range of the number of times a particular advertisement was shown in a selected location from the date it was first shown on that service. For privacy reasons, the impression ranges are published on a rolling basis after a delay of 90 days from the advertisement first being shown.</p>	
--	---	--

#### Audit procedures and information relied upon:

In order to evaluate the audited service's compliance with this DSA Specified Requirement, we primarily evaluated the design and operation of controls, as outlined below:

1. Conducted a walkthrough and inquired with management to gain an understanding of how the audited service's online repository included the advertisement information specified within this sub article.
2. Assessed the design of controls in place and determined that the suite of controls were appropriately designed and operating as intended. Inspected system configurations defined within the production code base and determined that the configurations were designed to include the following information within the Ads Transparency Center (ATC), when an advertisement was searched for:
  - (i) the content of the advertisement, including the name of the product, service or brand and the subject matter;
  - (ii) the advertiser name (per audited service's benchmark the natural or legal person on whose behalf the advertisement is presented is the same in all material instances as the natural or legal person who paid for the advertisement);
  - (iii) the period during which the advertisement was presented;
  - (iv) the main parameters used to present the advertisement specifically to one or more particular groups of recipients including, where applicable, the main parameters used to exclude such groups; and
  - (v) the total number of recipients the advertisement reached.





3. Independently searched for an advertisement within the ATC and determined that the ATC search results contained the advertiser information as described within this sub article. In addition, the audited service did not present information as to the “commercial communications presented on the platform as declared by the recipient of the service” as the content provided by recipients of the service is not and does not contain commercial communications as defined under DSA Article 3(w). For the period 1 June 2024 to 26 May 2025, “the natural or legal person who paid for the advertisement if different from the natural or legal person referred to in point (b)” was not explicitly presented in the ATC. To satisfy the requirement, the audited service obtained confirmation that the end-advertiser (i.e., the person on whose behalf the advertisement is presented) was the same as the person paying for the advertisement. This is because in all material respects, the end-advertiser is the person paying for the advertisement, and in situations where an end-advertiser is paying an advertising agency to place an advertisement, regardless of an agency intermediary, the end-advertiser is still the party paying for the advertisement since the advertising agency is being reimbursed by the end-advertiser. From 27 May 2025 onwards, the audited service included an additional “ad funded by” disclosure within the ATC when applicable to make it clearer to users the identity of the party paying for the advertisements.

4. Inspected relevant IT controls, including controls related to change management and logical access, for the relevant systems in the production environment and determined that the controls were in place throughout the DSA Examination Period to address the key IT risks.

5. Inquired with management and management noted that no significant changes were made to the policies, processes and/or controls after the walkthrough had been conducted through the end of the DSA Examination Period.

#### **Changes to the audit procedures during the audit:**

None.

#### **Results of procedures performed, how reasonable level of assurance was achieved, and conclusion:**

There were no material deviations identified in the performance of the above procedures, unless denoted below. The results of the audit procedures were deemed sufficient to obtain reasonable assurance.

**Positive** - In our opinion, the audited service complied with this DSA Specified Requirement during the DSA Examination Period, in all material respects.

#### **Recommendations on specific measures:**

Not applicable.

#### **Recommended timeframe to implement specific measures:**

Not applicable.

<b>Obligation:</b>	<b>Audit criteria:</b>	<b>Materiality threshold:</b>
39.3	<p>Throughout the period, in all material aspects:</p> <ol style="list-style-type: none"> <li>For advertisements that were removed or disabled based on alleged illegality or incompatibility with the provider terms and conditions, the repository did not include the following information: <ul style="list-style-type: none"> <li>- the content of the advertisement, including the name of the product, service or brand and the subject matter;</li> </ul> </li> </ol>	<p>If a control was not suitably designed and operated effectively to satisfy the obligation for at least 95% of the DSA Examination Period, and/or if there was an actual or projected error of more than 5% (or other material qualitative variance) during the DSA Examination Period related to the audit criteria.</p>



	<ul style="list-style-type: none"> <li>- the natural or legal person on whose behalf the advertisement is presented; or</li> <li>- the natural or legal person who paid for the advertisement, if that person is different from the person referred to in point above.</li> </ul> <p>2. For advertisements that were removed or disabled based on alleged illegality or incompatibility with the provider terms and conditions, the repository included the information from the statement of reasons referred to in Article 17.3, points (a) to (e), summarized below:</p> <ul style="list-style-type: none"> <li>- information on whether the decision entailed either the removal of, the disabling of access to, the demotion of or the restriction of the visibility of the information, or the suspension or termination of monetary payments related to that information, or imposes other measures referred to in Article 17.1 with regard to the information and where relevant, the territorial scope of the decision and its duration;</li> <li>- the facts and circumstances relied on in taking the decision including, where relevant, information on whether the decision was taken pursuant to a notice submitted under Article 16 or based on voluntary own-initiative investigations and, where strictly necessary, the identity of the notifier;</li> <li>- where applicable, information on the use made of automated means in taking the decision, including information on whether the decision was taken in respect of content detected or identified using automated means;</li> <li>- for allegedly illegal content, a reference to the legal ground relied on and explanation of why the information is considered to be illegal content on that ground;</li> <li>- for alleged incompatibility of the information with the terms and conditions of hosting services, a reference to the contractual grounds relied on and explanations as to why the information was considered to be incompatible with that ground;</li> </ul> <p>or Article 9.2, point (a)(i):</p> <ul style="list-style-type: none"> <li>- a reference to the legal basis under Union or national law for the order against illegal content.</li> </ul> <p><b>The following are certain operational benchmark(s) defined by the audited service:</b></p> <p>"the natural or legal person who paid for the advertisement if different from the natural or legal person referred to in point (b)": the audited service obtains confirmation that the end-advertiser (i.e., the person on whose behalf the</p>	
--	---	--



	<p>advertisement is presented) is the same as the person paying for the advertisement. This is because, in all material respects, the end-advertiser is the person paying for the advertisement, and in situations where an end-advertiser is paying an advertising agency to place an advertisement, regardless of an agency intermediary, the end-advertiser is still the party paying for the advertisement since the advertising agency is being reimbursed by the end-advertiser.</p>	
<p><b>Audit procedures and information relied upon:</b></p> <p>In order to evaluate the audited service's compliance with this DSA Specified Requirement, we primarily evaluated the design and operation of controls, as outlined below:</p> <ol style="list-style-type: none"> <li>1. Conducted a walkthrough and inquired with management to gain an understanding of how the audited service's online repository included the information from the statement of reasons (SOR) referred to in Article 17.3, points (a) to (e), for advertisements that were removed or disabled based on alleged illegality or incompatibility with the provider terms and conditions, and how the audited service's online repository did not include information about the content of the advertisement and the advertiser's name for such advertisements.</li> <li>2. Assessed the design of the control in place and determined that it was appropriately designed and operating as intended. Inspected the system configuration within the production code base and determined that jobs within the ATC were configured to trigger the movement of advertisement data from the 'active' to 'removed' section of the ATC databases when an SOR is received from the Ads Safety Platform (ASP). Thirty days after an SOR is received from the ASP (to deter bad actors from circumnavigating the audited service's enforcement strategy), the required details become publicly available in the 'removed' section of the ATC. Further determined that the ATC was configured to pull mandatory elements from the SOR for presentation into the ATC UI. For a sample advertisement where a SOR was issued, sampled in accordance with the sampling approach described in Appendix 2, inspected evidence of the job logs and determined that the job to move advertisement data from the 'active' to 'removed' section of the ATC databases was appropriately triggered to move the advertisement data from the 'active' to the 'removed' section of the ATC databases. Inspected the advertisement data presented in the ATC UI repository for the same advertisement sampled and determined that it included mandatory SOR elements such that: <ul style="list-style-type: none"> <li>- information described in Article 39.2, points (a) and (b) had been removed</li> <li>- information described in Article 39.2, points (d), (e), (g) and</li> <li>- information referred to in Article 17.3, points (a) to (e) were presented.</li> </ul> </li> <li>3. Inspected evidence and determined that the audited service had not received any orders in accordance with Article 9.2(a)(i), during the DSA Examination Period. As such, there were no advertisements presented within the ATC that included the information referred to in Article 9.2(a)(i).</li> <li>4. Inspected relevant IT controls, including controls related to change management and logical access, for the relevant systems in the production environment and determined that the controls were in place throughout the DSA Examination Period to address the key IT risks.</li> </ol>		



5. Inquired with management and management noted that no significant changes were made to the policies, processes and/or controls after the walkthrough had been conducted through the end of the DSA Examination Period.

**Changes to the audit procedures during the audit:**

None.

**Results of procedures performed, how reasonable level of assurance was achieved, and conclusion:**

There were no material deviations identified in the performance of the above procedures, unless denoted below. The results of the audit procedures were deemed sufficient to obtain reasonable assurance.

**Positive** - In our opinion, the audited service complied with this DSA Specified Requirement during the DSA Examination Period, in all material respects.

**Recommendations on specific measures:**

Not applicable.

**Recommended timeframe to implement specific measures:**

Not applicable.

Obligation:	Audit criteria:	Materiality threshold:
40.1	<p>Throughout the period, in all material aspects:</p> <p>Access to data necessary to monitor and assess compliance with the DSA was provided at the reasoned request of the Digital Services Coordinator of establishment or the Commission, within a reasonable period of time specified in the request.</p>	<p>If a control was not suitably designed and operated effectively to satisfy the obligation for at least 95% of the DSA Examination Period, and/or if there was an actual or projected error of more than 5% (or other material qualitative variance) during the DSA Examination Period related to the audit criteria.</p>

**Audit procedures and information relied upon:**

In order to evaluate the audited service's compliance with this DSA Specified Requirement, we evaluated the design and operation of controls and performed substantive procedures, as outlined below:

1. Conducted a walkthrough and inquired with management to gain an understanding of the audited service's process for providing access to data to the Digital Services Coordinator of establishment (DSC) or the Commission within the period of time specified in the request.
2. Based on our walkthrough and inquiries of management, determined that there were no requests received from the DSC or the Commission. To corroborate this, inspected system screenshots from the internal tool where requests for access submitted in accordance with Article 40.1 are tracked and determined that there were no data access requests received from the DSC or the Commission during the DSA Examination Period.
3. To validate that the audited service was prepared to intake and respond to requests submitted by the DSC or the Commission, inspected the DSA Point of Contact public website, and determined that the DSC or the Commission has



a means to submit requests for access to data pursuant to Article 40.1 using an application form that is submitted through the website.

4. Inspected relevant IT controls, including controls related to change management and logical access, for the relevant systems in the production environment and determined that the controls were in place throughout the DSA Examination Period to address the key IT risks.

5. Inquired with management and management noted that no significant changes were made to the policies, processes and/or controls after the walkthrough had been conducted through the end of the DSA Examination Period.

**Changes to the audit procedures during the audit:**

None.

**Results of procedures performed, how reasonable level of assurance was achieved, and conclusion:**

There were no material deviations identified in the performance of the above procedures, unless denoted below. The results of the audit procedures were deemed sufficient to obtain reasonable assurance.

**Positive** - In our opinion, the audited service complied with this DSA Specified Requirement during the DSA Examination Period, in all material respects.

**Recommendations on specific measures:**

Not applicable.

**Recommended timeframe to implement specific measures:**

Not applicable.

Obligation:	Audit criteria:	Materiality threshold:
40.12	<p>Throughout the period, in all material aspects:</p> <ol style="list-style-type: none"> <li>1. Access to data was provided to researchers, including those affiliated to not for profit bodies, organizations and associations, who comply with the conditions set out in Article 40.8, points (b), (c), (d) and (e), and who will use the data solely for performing research that contributes to the detection, identification and understanding of systemic risks in the Union pursuant to Article 34.1.</li> <li>2. Access to data was provided without undue delay.</li> <li>3. Access to real-time data was provided where technically possible.</li> </ol>	<p>If a control was not suitably designed and operated effectively to satisfy the obligation for at least 95% of the DSA Examination Period, and/or if there was an actual or projected error of more than 5% (or other material qualitative variance) during the DSA Examination Period related to the audit criteria.</p>



	<p><b>The following are certain operational benchmark(s) defined by the audited service:</b></p> <p>"undue delay": the audited service usually provides access within 15-30 days unless special circumstances require an in-depth analysis. Special circumstances may include circumstances requiring a more in-depth analysis into the merits of the data access application given the nature of the data requested, the scope of the proposed research project, and the qualifications of the research applicant (e.g., applications raising heightened concerns over the disclosure of private, sensitive, or confidential information, or where further investigation is needed into whether the applicant meets the conditions set out in Article 40.8, points (b), (c), (d) and (e)).</p>	
<p><b>Audit procedures and information relied upon:</b></p> <p>In order to evaluate the audited service's compliance with this DSA Specified Requirement, we evaluated the design and operation of controls and performed substantive procedures, as outlined below:</p> <ol style="list-style-type: none"> <li>1. Conducted a walkthrough and inquired with management and determined they have taken the necessary technical and organizational measures to handle access to data requested by researchers in accordance with Article 40, where applicable.</li> <li>2. Assessed the design of the policies and processes in place and determined that the policies and processes, and suite of controls in place were appropriately designed and operated as intended. Inspected the audited service's public facing Transparency site and determined that it included information about research options and an application form that researchers can use to apply for data access. Additionally, determined that an Acceptable Use Policy was available and must be agreed to by the applicant prior to submitting their application.</li> </ol> <p>Inspected the Internal Runbook for DSA Research Public Data Project and determined that it defined a process in place for relevant audited service personnel to review the intake form submitted by the researcher and determine, by assessing and authenticating evidence provided in the intake form, if the researcher is compliant with all established criteria for data access in accordance with Article 40.8, points (b), (c), (d), and (e), with additional evaluation from the audited service's working group if necessary.</p> <p>Selected a sample of data access requests submitted during the DSA Examination Period, sampled in accordance with the sampling approach described in Appendix 2, to test whether a response and appropriate access to the data, if approved, was provided without undue delay. For the approved samples selected and tested, determined that access was provided within 15 - 30 days of the application submission date. Further determined that where access to real time data was technically possible, such access was provided to the approved researcher.</p> <ol style="list-style-type: none"> <li>3. Inspected the Acceptable Use Policy and determined that the policy is appropriate and in line with the provision requirements.</li> <li>4. Selected a sample of requests received from research applicants, sampled in accordance with the sampling approach described in Appendix 2. Inspected the documentation filled out by the team member reviewing the data access requests within the internal tracking tool and determined that the documentation included an assessment</li> </ol>		



against the conditions defined under Article 40.8, points (b), (c), (d), and (e), to provide access to data to researchers who comply with these conditions, with additional evaluation from the audited service's working group if necessary.

5. Inspected relevant IT controls, including controls related to change management and logical access, for the relevant systems in the production environment and determined that the controls were in place throughout the DSA Examination Period to address the key IT risks.

6. Inquired with management and management noted that no significant changes were made to the policies, processes and/or controls after the walkthrough had been conducted through the end of the DSA Examination Period.

**Changes to the audit procedures during the audit:**

None.

**Results of procedures performed, how reasonable level of assurance was achieved, and conclusion:**

There were no material deviations identified in the performance of the above procedures, unless denoted below. The results of the audit procedures were deemed sufficient to obtain reasonable assurance.

**Positive** - In our opinion, the audited service complied with this DSA Specified Requirement during the DSA Examination Period, in all material respects.

**Recommendations on specific measures:**

Not applicable.

**Recommended timeframe to implement specific measures:**

Not applicable.

<b>Obligation:</b>	<b>Audit criteria:</b>	<b>Materiality threshold:</b>
41.1	<p>Throughout the period, in all material aspects:</p> <p>The provider established a compliance function to monitor the compliance of the provider with the DSA which:</p> <ul style="list-style-type: none"> <li>- was independent from operational functions;</li> <li>- was composed of one or more compliance officers; including head of compliance function;</li> <li>- had sufficient authority, stature, and resources; and</li> <li>- had access to the management body.</li> </ul>	<p>If a control was not suitably designed and operated effectively to satisfy the obligation for at least 95% of the DSA Examination Period, and/or if there was an actual or projected error of more than 5% (or other material qualitative variance) during the DSA Examination Period related to the audit criteria.</p>

**Audit procedures and information relied upon:**

In order to evaluate the audited service's compliance with this DSA Specified Requirement, we performed substantive procedures, although controls existed, as outlined below:

1. Conducted a walkthrough and inquired with management to gain an understanding of the compliance function and determined it was comprised of more than one compliance officer and had a head of compliance function independent





from operational functions and had sufficient authority, stature, and resources, as well as access to the management body.

2. Assessed policy documentation and charters and determined they were appropriately in place to define the Independent Compliance Function (ICF) and its role, as well as its reporting requirements to the management body.

3. Inspected meeting agendas and excerpts of minutes where the management body reviewed the composition of the ICF and organization charts and determined the ICF was comprised of the head of compliance function and more than one compliance officer and have sufficient resources.

4. Inspected charters, job descriptions as well as the credentials of the members of the ICF and determined they were independent from operating functions and have sufficient authority, stature and resources to perform their duties.

5. Inspected meeting agendas and excerpts of minutes of the quarterly board meetings and ad hoc meetings and determined the ICF had access to the management body to raise concerns and inform it of the audited service's status of compliance with the DSA.

6. Inquired with management and management noted that no significant changes were made to the policies, processes and/or controls after the walkthrough had been conducted through the end of the DSA Examination Period.

**Changes to the audit procedures during the audit:**

None.

**Results of procedures performed, how reasonable level of assurance was achieved, and conclusion:**

There were no material deviations identified in the performance of the above procedures, unless denoted below. The results of the audit procedures were deemed sufficient to obtain reasonable assurance.

**Positive** - In our opinion, the audited service complied with this DSA Specified Requirement during the DSA Examination Period, in all material respects.

**Recommendations on specific measures:**

Not applicable.

**Recommended timeframe to implement specific measures:**

Not applicable.

Obligation:	Audit criteria:	Materiality threshold:
41.2	<p>Throughout the period, in all material aspects:</p> <ol style="list-style-type: none"> <li>1. A management body of the provider has ensured the following: <ul style="list-style-type: none"> <li>- that compliance officers had the professional qualifications, knowledge, experience and ability necessary to fulfil the tasks set out in Article 41.3; and</li> <li>- that the head of the compliance function was an</li> </ul> </li> </ol>	<p>If a control was not suitably designed and operated effectively to satisfy the obligation for at least 95% of the DSA Examination Period, and/or if there was an actual or projected error of more than 5% (or other material qualitative variance) during the DSA Examination Period related to the audit criteria.</p>





	<p>independent senior manager with distinct responsibility for the compliance function.</p> <p>2. The head of the compliance function reported directly to the management body and could raise concerns and warn that body regarding risks referred to in Articles 34 or non-compliance with the DSA which could have affected the provider.</p> <p>3. The head of the compliance function was not removed without prior approval of the management body.</p>	
<p><b>Audit procedures and information relied upon:</b></p> <p>In order to evaluate the audited service's compliance with this DSA Specified Requirement, we performed substantive procedures, although controls existed, as outlined below:</p> <ol style="list-style-type: none"> <li>1. Conducted a walkthrough and inquired with management to gain an understanding of how the management body (Google Ireland Limited Board of Directors) oversees the compliance function and its procedures in monitoring the compliance of the audited service with the DSA, ensuring the compliance officers and the head of compliance function have the professional qualifications, knowledge, experience and ability necessary to fulfil their tasks.</li> <li>2. Assessed policy documentation and determined that the head of the compliance function cannot be removed without prior approval of the management body and has been in their role for the duration of the DSA Examination Period. Inspected the Head Compliance Officer replacement related documents and determined that the replacement was approved by the management body and carried out in accordance with the documented policy.</li> <li>3. Assessed that policy documentation and charters were appropriately in place to designate the management body and define its role in providing oversight of the ICF to ensure the ICF was independent, effective, and accountable for complying with applicable regulations.</li> <li>4. Inspected meeting agendas and excerpts of minutes of the quarterly board meetings and ad hoc meetings and determined the head of the compliance function reported directly to the management body and could raise any concerns and warn the management body regarding risks referred to in Articles 34 or non-compliance with the DSA which could have affected the audited service.</li> <li>5. Inspected job descriptions as well as the credentials of the members of the ICF and determined they are independent from operating functions and have the professional qualifications, knowledge, experience and ability necessary to fulfill the tasks outlined in Article 41.3. Additionally, inspected the charter and determined the head of the compliance function is an independent role with distinct responsibility for the compliance function.</li> <li>6. Inquired with management and management noted that no significant changes were made to the policies, processes and/or controls after the walkthrough had been conducted through the end of the DSA Examination Period.</li> </ol> <p><b>Changes to the audit procedures during the audit:</b></p> <p>None.</p>		


**Results of procedures performed, how reasonable level of assurance was achieved, and conclusion:**

There were no material deviations identified in the performance of the above procedures, unless denoted below. The results of the audit procedures were deemed sufficient to obtain reasonable assurance.

**Positive** - In our opinion, the audited service complied with this DSA Specified Requirement during the DSA Examination Period, in all material respects.

**Recommendations on specific measures:**

Not applicable.

**Recommended timeframe to implement specific measures:**

Not applicable.

Obligation:	Audit criteria:	Materiality threshold:
41.3	<p>Throughout the period, in all material aspects:</p> <p>The compliance officers engaged in the following tasks:</p> <ul style="list-style-type: none"> <li>(a) cooperated with the Digital Services Coordinator of establishment and the Commission;</li> <li>(b) ensured that all risks referred to in Article 34 were identified and properly reported on and that reasonable, proportionate and effective risk-mitigation measures were taken pursuant to Article 35;</li> <li>(c) organized and supervised the independent audit activities pursuant to Article 37;</li> <li>(d) informed and advised management and employees about relevant obligations under the DSA;</li> <li>(e) monitored the compliance of the audited service with its obligations under the DSA; and</li> <li>(f) where applicable, monitored the compliance with commitments made under the codes of conduct pursuant to Articles 45 and 46 or the crisis protocols pursuant to Article 48.</li> </ul> <p><b>The following are certain operational benchmark(s) defined by the audited service:</b></p> <p>“reasonable, proportionate, effective measures”: mitigation measures / action plans put in place to address systemic risks identified during the risk assessment in areas of heightened residual risk (can be tied to OKRs, Launches, Programs, etc.) and – combined with the suite of other relevant mitigations – have the effect of lessening (or keeping stable) levels of systemic risk while being commensurate to the</p>	<p>If a control was not suitably designed and operated effectively to satisfy the obligation for at least 95% of the DSA Examination Period, and/or if there was an actual or projected error of more than 5% (or other material qualitative variance) during the DSA Examination Period related to the audit criteria.</p>



	severity and probability, recognizing that external factors are dynamic and may change.	
<p><b>Audit procedures and information relied upon:</b></p> <p>In order to evaluate the audited service's compliance with this DSA Specified Requirement, we performed substantive procedures, although controls existed, as outlined below:</p> <ol style="list-style-type: none"> <li>1. Conducted a walkthrough and inquired with management to gain an understanding of how the Independent Compliance Function (ICF) cooperated with the Digital Services Coordinator of establishment and the Commission, performed an independent assessment of the Systemic Risk Assessment (SRA) process related to Article 34 and 35, assisted in the organization and supervision of the independent audit activities pursuant to Article 37, informed management and employees about relevant obligations under the DSA via training modules, and monitored the compliance of the audited service with its obligations under the DSA.</li> <li>2. Assessed that policy documentation and charters were appropriately in place for the compliance officers to be responsible for the tasks outlined in Article 41.3(a) through 41.3(e).</li> <li>3. Inspected relevant correspondence and determined the ICF cooperated with the Digital Services Coordinator of establishment and the Commission during the DSA Examination Period.</li> <li>4. Inspected the weekly ICF meeting agenda and excerpts of minutes of quarterly board meetings which demonstrate the procedures performed by the ICF during its independent 2024 SRA assessment and determined the ICF assessed that the risks referred to in Article 34 were identified and properly reported on, and that mitigation measures are in the process of being implemented under Article 35 with certain mitigation measures already implemented and evaluated under Article 34.</li> </ol> <p>Additionally, obtained and reviewed the results of the independent 2024 SRA assessment performed by the ICF were presented to the management body and 2024 SRA team. To corroborate the aforementioned procedures performed by the ICF, inquired with the head compliance officer and confirmed that the ICF actively monitored the audited service's compliance with the DSA, including Articles 34 and 35, throughout the DSA Examination Period.</p> <ol style="list-style-type: none"> <li>5. Inspected the agendas and meeting minutes of weekly ICF meetings and quarterly board meetings and determined the ICF organized and supervised the activities of the independent audit pursuant to Article 37. Additionally, validated via inspection of the ICF email communications to the management body that the ICF monitored the audit progress and provided regular status updates to the management body.</li> <li>6. Inspected training materials and determined the ICF maintains and distributes the training materials to management and employees of the audited service to inform them of relevant obligations under the DSA.</li> <li>7. Inspected the compliance monitoring plan and determined the ICF had a process to monitor the compliance of the audited service with its obligations under the DSA through performing internal controls validation and validation of completed remediation. To corroborate the aforementioned procedures performed by the ICF, inquired with the head compliance officer and confirmed that the ICF actively monitored the audited service's compliance with its obligations under the DSA, throughout the DSA Examination Period. Additionally, inspected the agendas and excerpts of meeting minutes of quarterly board meetings and ad hoc meetings, and determined the compliance monitoring plan had been reviewed and approved by the management body, and ICF provided status updates on the control validation process to demonstrate their monitoring of the compliance of the audited service with its obligations.</li> </ol>		



8. Inquired with management and management noted that no significant changes were made to the policies, processes and/or controls after the walkthrough had been conducted through the end of the DSA Examination Period.

**Changes to the audit procedures during the audit:**

None.

**Results of procedures performed, how reasonable level of assurance was achieved, and conclusion:**

There were no material deviations identified in the performance of the above procedures, unless denoted below. The results of the audit procedures were deemed sufficient to obtain reasonable assurance.

**Positive** - In our opinion, the audited service complied with this DSA Specified Requirement during the DSA Examination Period, in all material respects.

**Recommendations on specific measures:**

Not applicable.

**Recommended timeframe to implement specific measures:**

Not applicable.

Obligation:	Audit criteria:	Materiality threshold:
41.4	<p>Throughout the period, in all material aspects:</p> <p>The provider communicated the name and contact details of the head of the compliance function to the Digital Services Coordinator of establishment and to the Commission.</p>	<p>If a control was not suitably designed and operated effectively to satisfy the obligation for at least 95% of the DSA Examination Period, and/or if there was an actual or projected error of more than 5% (or other material qualitative variance) during the DSA Examination Period related to the audit criteria.</p>

**Audit procedures and information relied upon:**

In order to evaluate the audited service's compliance with this DSA Specified Requirement, we performed substantive procedures, although controls existed, as outlined below:

1. Conducted a walkthrough and inquired with management regarding the process to communicate the name and contact details of the head of the compliance function to the Digital Services Coordinator of establishment and to the Commission.
2. Inspected email correspondence and determined the provider communicated the name and contact details of the head of the compliance function to the Digital Services Coordinator of establishment and to the Commission at the start of the DSA Examination Period.
3. Inquired with management and management noted that no significant changes were made to the policies, processes and/or controls after the walkthrough had been conducted through the end of the DSA Examination Period.


**Changes to the audit procedures during the audit:**

None.

**Results of procedures performed, how reasonable level of assurance was achieved, and conclusion:**

There were no material deviations identified in the performance of the above procedures, unless denoted below. The results of the audit procedures were deemed sufficient to obtain reasonable assurance.

**Positive** - In our opinion, the audited service complied with this DSA Specified Requirement during the DSA Examination Period, in all material respects.

**Recommendations on specific measures:**

Not applicable.

**Recommended timeframe to implement specific measures:**

Not applicable.

**Obligation:**

41.5

**Audit criteria:**

Throughout the period, in all material aspects:

The management body of the provider defined, oversaw, and remains accountable for the implementation of the provider's governance arrangements to ensure the independence of the compliance function, including the division of responsibilities within the organization, the prevention of conflicts of interest, and management of systemic risks identified pursuant to Article 34.

**Materiality threshold:**

If a control was not suitably designed and operated effectively to satisfy the obligation for at least 95% of the DSA Examination Period, and/or if there was an actual or projected error of more than 5% (or other material qualitative variance) during the DSA Examination Period related to the audit criteria.

**Audit procedures and information relied upon:**

In order to evaluate the audited service's compliance with this DSA Specified Requirement, we performed substantive procedures, as outlined below:

1. Conducted a walkthrough and inquired with management to gain an understanding of how the management body of the provider defined, oversaw, and maintained accountability for the implementation of the audited provider's governance arrangements to ensure the independence of the compliance function, including the division of responsibilities, the prevention of conflicts of interest, and management of systemic risks identified pursuant to Article 34, as part of the annual, independent Systemic Risk Assessment (SRA) framework that was designed and implemented by the compliance function during the DSA Examination Period.
2. Inspected and assessed that policy documentation and the framework for the Independent Compliance Function's (ICF) independent assessment of the audited service's 2024 SRA was appropriately in place to comply with the DSA Specified Requirements.



3. Inspected meeting agendas and excerpts of minutes of the board meetings and ad hoc meetings and determined the management body oversaw the ICF throughout the DSA Examination Period to ensure the ICF is independent of the 2024 SRA process, there were no conflicts of interest, and the risks identified pursuant to Article 34 were assessed by the ICF.

4. Inspected the procedures performed by the ICF during its 2024 SRA assessment and determined the ICF assessed that the risks referred to in Article 34 were identified and properly reported on. Additionally, noted that the results of the independent 2024 SRA assessment performed by the ICF were presented to the management body and 2024 SRA team.

5. Inquired with management and management noted that no significant changes were made to the policies, processes and/or controls after the walkthrough had been conducted through the end of the DSA Examination Period.

**Changes to the audit procedures during the audit:**

None.

**Results of procedures performed, how reasonable level of assurance was achieved, and conclusion:**

There were no material deviations identified in the performance of the above procedures, unless denoted below. The results of the audit procedures were deemed sufficient to obtain reasonable assurance.

**Positive** - In our opinion, the audited service complied with this DSA Specified Requirement during the DSA Examination Period, in all material respects.

**Recommendations on specific measures:**

Not applicable.

**Recommended timeframe to implement specific measures:**

Not applicable.

<p><b>Obligation:</b></p> <p>41.6</p>	<p><b>Audit criteria:</b></p> <p>Throughout the period, in all material aspects:</p> <p>The management body reviewed and approved, at least once a year, the strategies and policies for taking up, managing, monitoring and mitigating the risks identified pursuant to Article 34.</p>	<p><b>Materiality threshold:</b></p> <p>If a control was not suitably designed and operated effectively to satisfy the obligation for at least 95% of the DSA Examination Period, and/or if there was an actual or projected error of more than 5% (or other material qualitative variance) during the DSA Examination Period related to the audit criteria.</p>
<p><b>Audit procedures and information relied upon:</b></p> <p>In order to evaluate the audited service's compliance with this DSA Specified Requirement, we performed substantive procedures, as outlined below:</p>		



1. Conducted a walkthrough and inquired with management to gain an understanding of how the management body reviewed and approved the strategies and policies in place for taking up, managing, monitoring and mitigation of the risks identified pursuant to Article 34.
2. Assessed that policy documentation such as charters and assessment frameworks were appropriately in place prior to the start of the DSA Examination Period to comply with the DSA Specified Requirements.
3. Inspected meeting agendas and excerpts of minutes of the quarterly board meetings and ad hoc meetings and determined that the management body reviewed and approved the 2024 SRA assurance plan presented by the ICF during the DSA Examination Period that included the strategies and policies for taking up, managing, monitoring and mitigating the risks pursuant to Article 34.
4. Inspected the procedures performed by the ICF during its 2024 SRA assessment and determined the ICF assessed that the risks referred to in Article 34 were identified and properly reported on and mitigation measures are in the process of being implemented pursuant to Article 35, with certain mitigation measures already implemented and evaluated under Article 34. Additionally, the results of the independent 2024 SRA assessment performed by the ICF were presented to the management body and 2024 SRA team during the DSA Examination Period.
5. Inquired with management and management noted that no significant changes were made to the policies, processes and/or controls after the walkthrough had been conducted through the end of the DSA Examination Period.

**Changes to the audit procedures during the audit:**

None.

**Results of procedures performed, how reasonable level of assurance was achieved, and conclusion:**

There were no material deviations identified in the performance of the above procedures, unless denoted below. The results of the audit procedures were deemed sufficient to obtain reasonable assurance.

**Positive** - In our opinion, the audited service complied with this DSA Specified Requirement during the DSA Examination Period, in all material respects.

**Recommendations on specific measures:**

Not applicable.

**Recommended timeframe to implement specific measures:**

Not applicable.

<b>Obligation:</b>	<b>Audit criteria:</b>	<b>Materiality threshold:</b>
41.7	<p>Throughout the period, in all material aspects:</p> <p>The management body:</p> <ul style="list-style-type: none"> <li>- devoted sufficient time to the consideration of the measures related to risk management;</li> <li>- maintained active involvement in the decisions related to risk management; and</li> <li>- ensured that adequate resources were allocated to</li> </ul>	<p>If a control was not suitably designed and operated effectively to satisfy the obligation for at least 95% of the DSA Examination Period, and/or if there was an actual or projected error of more than 5% (or other material qualitative variance) during the DSA Examination Period related to the audit criteria.</p>





	<p>the management of the risks identified in accordance with Article 34.</p> <p><b>The following are certain operational benchmark(s) defined by the audited service:</b></p> <p>“active involvement”: the GIL board is regularly informed about DSA risk management decisions and processes, has the opportunity to consider, raise queries, and input on the strategies and measures taken to address such risks.</p> <p>“sufficient time”: the GIL board ensures time is available as required at its scheduled meetings to discuss DSA risk management and is available for out of cadence meetings as required.</p>	
--	--	--

#### **Audit procedures and information relied upon:**

In order to evaluate the audited service’s compliance with this DSA Specified Requirement, we performed substantive procedures, as outlined below:

1. Conducted a walkthrough and inquired with management to gain an understanding of how the management body oversaw the compliance function and its procedures in monitoring the compliance of the audited service with the DSA throughout the DSA Examination Period.
2. Assessed that policy documentation and charters were appropriately in place to comply with the DSA Specified Requirements.
3. Inspected meeting agendas and excerpts of minutes of the quarterly board meetings and ad hoc meetings and determined the management body devoted sufficient time to the consideration of the measures related to risk management, maintained active involvement in the decisions related to risk management, and ensured that adequate resources were allocated to the management of the risks identified in accordance with Article 34 as part of the Independent Compliance Function’s (ICF) independent 2024 SRA assessment. Evaluated the sufficiency of time devoted by the management body considering the ad hoc meetings scheduled between the compliance function and management body throughout the DSA Examination Period, in addition to their quarterly meetings, which we determined to be reasonable. To corroborate the aforementioned procedures performed by the ICF, inquired with the management board and confirmed that the management body devoted sufficient time during the scheduled board meetings to DSA risk management decisions and processes and was actively involved in the decisions related to risk management.
4. Inquired with management and management noted that no significant changes were made to the policies, processes and/or controls after the walkthrough had been conducted through the end of the DSA Examination Period.

#### **Changes to the audit procedures during the audit:**

None.

#### **Results of procedures performed, how reasonable level of assurance was achieved, and conclusion:**





There were no material deviations identified in the performance of the above procedures, unless denoted below. The results of the audit procedures were deemed sufficient to obtain reasonable assurance.

**Positive** - In our opinion, the audited service complied with this DSA Specified Requirement during the DSA Examination Period, in all material respects.

**Recommendations on specific measures:**

Not applicable.

**Recommended timeframe to implement specific measures:**

Not applicable.

**Obligation:**

42.1

**Audit criteria:**

Throughout the period, in all material aspects:

The provider published transparency reports referred to in Article 15:

- no later than two months from the date of application referred to in Article 33.6, second subparagraph, and
- at least every six months thereafter.

**Materiality threshold:**

If a control was not suitably designed and operated effectively to satisfy the obligation for at least 95% of the DSA Examination Period, and/or if there was an actual or projected error of more than 5% (or other material qualitative variance) during the DSA Examination Period related to the audit criteria.

**Audit procedures and information relied upon:**

In order to evaluate the audited service's compliance with this DSA Specified Requirement, we performed substantive procedures, although controls existed, as outlined below:

1. Conducted a walkthrough and inquired with management to gain an understanding of the process for publishing transparency reports to the publicly accessible Google Transparency Report PDF Download Centre (publicly accessible portal where a user can download various reports published by the provider).
2. Inspected the Google Transparency Report PDF Download Centre and verified that the Article 15 transparency reports were published at least every six months, with the transparency reports being published on 28 August 2024 and 28 February 2025.
3. Inquired with management and management noted that no significant changes were made to the policies, processes and/or controls after the walkthrough had been conducted through the end of the DSA Examination Period.

**Changes to the audit procedures during the audit:**

None.

**Results of procedures performed, how reasonable level of assurance was achieved, and conclusion:**

There were no material deviations identified in the performance of the above procedures, unless denoted below. The results of the audit procedures were deemed sufficient to obtain reasonable assurance.



**Positive** – In our opinion, the audited service complied with this DSA Specified Requirement during the DSA Examination Period, in all material respects.

**Recommendations on specific measures:**

Not applicable.

**Recommended timeframe to implement specific measures:**

Not applicable.

**Obligation:**

42.3

**Audit criteria:**

Throughout the period, in all material aspects:

The provider included in the transparency reports referred to in Article 42.1 the average monthly active recipients of the service for each member state.

**The following are certain operational benchmark(s) defined by the audited service:**

“monthly active recipient”:  
recipients in a signed in or signed out state, including business users, in the EU and having engaged at least once per 28 days/month on all surfaces where recipients can interact with the service and as further explained in the Overview and Additional Notes section of the MAR reports.

**Materiality threshold:**

If a control was not suitably designed and operated effectively to satisfy the obligation for at least 95% of the DSA Examination Period, and/or if there was an actual or projected error of more than 5% (or other material qualitative variance) during the DSA Examination Period related to the audit criteria.

**Audit procedures and information relied upon:**

In order to evaluate the audited service's compliance with this DSA Specified Requirement, we evaluated the design and operation of controls and performed substantive procedures, as outlined below:

1. Conducted a walkthrough and inquired with management to gain an understanding of the process used for determining signed-in and signed-out recipients and the process for performing metric validation procedures prior to publication of the Monthly Active Recipients (MAR) Report.
2. Inspected methodology used for calculating the average monthly active recipients of the service in the Union and validated through reperformance of the calculations that the information was calculated as an average over a period of the past six months.
3. Inspected the Metric Validation Scorecard and the related tickets for approvals and confirmed that all of the metrics published in the MAR Reports during the DSA Examination Period have been validated by the Trust & Safety team, including a verification of the script used to pull recipient count data for the audited service from the correct data sources. Verified that the scorecard review was completed prior to report publication via a live walkthrough of all stakeholder approval dates. Validated that all approving stakeholders were appropriate based on their job functions/titles.



4. Inspected the published transparency report during the DSA Examination Period and validated that the average monthly active recipients of the service for each member state were included within the MAR Report and included data for each member state.
5. Inspected user access lists and confirmed the individuals that have access to modify the scripts to pull user count data for the audited service are appropriate based on their job title/function.
6. Inspected relevant IT controls, including controls related to change management and logical access, for the relevant systems in the production environment and determined that the controls were in place throughout the DSA Examination Period to address key IT risks.
7. Inquired with management and management noted that no significant changes were made to the policies, processes and/or controls after the walkthrough had been conducted through the end of the DSA Examination Period.

**Changes to the audit procedures during the audit:**

None.

**Results of procedures performed, how reasonable level of assurance was achieved, and conclusion:**

There were no material deviations identified in the performance of the above procedures, unless denoted below. The results of the audit procedures were deemed sufficient to obtain reasonable assurance.

**Positive** – In our opinion, the audited service complied with this DSA Specified Requirement during the DSA Examination Period, in all material respects.

**Recommendations on specific measures:**

Not applicable.

**Recommended timeframe to implement specific measures:**

Not applicable.

Obligation:	Audit criteria:	Materiality threshold:
42.4	<p>Throughout the period, in all material aspects:</p> <ol style="list-style-type: none"> <li>1. The provider transmitted the reports and other information specified in Article 42.4 to the Digital Services Coordinator of establishment and the Commission after the receipt of each audit report pursuant to Article 37.4, without undue delay upon completion.</li> <li>2. The provider made the reports specified in Article 42.4, publicly available at the latest three months after the receipt of each audit report pursuant to Article 37.4.</li> </ol>	<p>If a control was not suitably designed and operated effectively to satisfy the obligation for at least 95% of the DSA Examination Period, and/or if there was an actual or projected error of more than 5% (or other material qualitative variance) during the DSA Examination Period related to the audit criteria.</p>



### Audit procedures and information relied upon:

In order to evaluate the audited service's compliance with this DSA Specified Requirement, we performed substantive procedures, although controls existed, as outlined below:

1. Conducted a walkthrough and inquired with management to gain an understanding of the process for how the audited service provider transmitted the reports and other information specified in Article 42.4 to the Digital Services Coordinator (DSC) of establishment and the Commission after the receipt of each audit report pursuant to Article 37.4, without undue delay upon completion, and the process for how the audited service provider made the aforementioned reports publicly available at the latest three months after the receipt of each audit report pursuant to Article 37.4.
2. Inspected communications between the audited provider, the DSC, and the Commission and identified the dates when the following reports as specified in Article 42.4 were transmitted to the DSC and the Commission:
  - Report on Systemic Risk Assessments, including the specific mitigation measures put in place pursuant to Article 35.1, and information about the consultations conducted by the provider in support of the risk assessments and design of the risk mitigation measures, pursuant to Article 34.1 was completed and transmitted on 28 August 2024;
  - DSA Audit Report provided for in Article 37.4 was transmitted on 29 September 2024, two days post issuance of the report;
  - DSA Audit Implementation Report provided for in Article 37.6 was completed and transmitted on 27 October 2024. Compared the transmitted date for each report above with the receipt date of the audit report pursuant to Article 37.4 of 27 September 2024 and determined that the reports were transmitted to the DSC and the Commission without undue delay.
3. Inspected the PDF Download Center on the Transparency Center where the audited service provider published the reports and other information as specified in Article 42.4 and determined that the reports are publicly available. Compared the published date of 28 November 2024 for the reports to the receipt date of 27 September 2024 for the audit report pursuant to Article 37.4 and verified that the reports were published within three months after the receipt date of the audit report.
4. Inquired with management and management noted that no significant changes were made to the policies, processes and/or controls after the walkthrough had been conducted through the end of the DSA Examination Period.

### Changes to the audit procedures during the audit:

None.

### Results of procedures performed, how reasonable level of assurance was achieved, and conclusion:

There were no material deviations identified in the performance of the above procedures, unless denoted below. The results of the audit procedures were deemed sufficient to obtain reasonable assurance.

**Positive** – In our opinion, the audited service complied with this DSA Specified Requirement during the DSA Examination Period, in all material respects.



<b>Recommendations on specific measures:</b>  Not applicable.	<b>Recommended timeframe to implement specific measures:</b>  Not applicable.
---	---

<b>Obligation:</b>  42.5	<b>Audit criteria:</b>  Throughout the period, in all material aspects:  The provider transmitted the complete reports pursuant to Article 42.4, to the Digital Services Coordinator of establishment and the Commission, accompanied by a statement of reasons for removing information from the publicly available reports, where the provider removed information on the basis that the publication of such information might:  <ul style="list-style-type: none"> <li>- result in disclosure of confidential information of the provider or of the recipients of the service;</li> <li>- cause significant vulnerabilities for the security of its service; or</li> <li>- undermine public security or harm recipients.</li> </ul>	<b>Materiality threshold:</b>  If a control was not suitably designed and operated effectively to satisfy the obligation for at least 95% of the DSA Examination Period, and/or if there was an actual or projected error of more than 5% (or other material qualitative variance) during the DSA Examination Period related to the audit criteria.
--------------------------------	--	---

#### Audit procedures and information relied upon:

In order to evaluate the audited service's compliance with this DSA Specified Requirement, we performed substantive procedures, as outlined below:

1. Conducted a walkthrough and inquired with management to gain an understanding of the process for how the audited service provider transmitted the complete reports pursuant to Article 42.4 to the Digital Services Coordinator (DSC) of establishment and the Commission, identified and removed information from the publicly available reports, and transmitted a statement of reasons for removing such information to the DSC and the Commission.
2. Inspected the communications between the audited provider, the DSC, and the Commission and verified that the complete reports pursuant to Article 42.4 were transmitted to both the DSC and the Commission, accompanied by a statement of reasons for removing information from the publicly available reports on 28 November 2024, the same date that the reports were made publicly available.
3. Compared the publicly available reports with the complete, unredacted version of the reports submitted to the DSC and to the Commission and identified the instances where information was removed from the publicly available versions. Compared the information removed from the publicly available versions of the reports against the statement of reasons submitted by the audited service provider and verified that the audited service provider had included all removals and an explanation for the removals in their statement of reasons.
4. Inspected the statement of reasons submitted by the audited service provider and for each piece of information removed from the publicly available reports, determined that the audited provider removed the information on the basis



<p>that such information might result in disclosure of confidential information of the provider or of the recipients of the service, cause significant vulnerabilities for the security of its service, or undermine public security or harm recipients.</p> <p>5. Inquired with management and management noted that no significant changes were made to the policies, processes and/or controls after the walkthrough had been conducted through the end of the DSA Examination Period.</p> <p><b>Changes to the audit procedures during the audit:</b></p> <p>None.</p> <p><b>Results of procedures performed, how reasonable level of assurance was achieved, and conclusion:</b></p> <p>There were no material deviations identified in the performance of the above procedures, unless denoted below. The results of the audit procedures were deemed sufficient to obtain reasonable assurance.</p> <p><b>Positive</b> – In our opinion, the audited service complied with this DSA Specified Requirement during the DSA Examination Period, in all material respects.</p>	
<p><b>Recommendations on specific measures:</b></p> <p>Not applicable.</p>	<p><b>Recommended timeframe to implement specific measures:</b></p> <p>Not applicable.</p>



## Appendix 2 – Overview of methodology/approach of procedures performed

### Overview

As part of determining the initial risk assessment for each obligation (or shortly thereafter), we made inquiries and/or performed a walkthrough of applicable processes or controls to obtain a sufficient understanding in order to design the nature, timing and extent of our procedures to obtain reasonable assurance.

For each obligation we took one of the following approaches:

1. *Primarily evaluated the design and operation of control(s).* If the audited provider has a control or set of controls that closely aligns with the relevant DSA Specified Requirements, we executed procedures to assess the design and operation of the control and did not perform substantive procedures other than inquiry (unless denoted otherwise).
2. *Performed substantive procedures, although control(s) existed.* If the audited provider has a control or set of controls that closely aligns with the relevant DSA Specified Requirements, but we deemed assessment to be more efficient by executing substantive procedures, we executed substantive procedures and did not perform procedures to assess the design and operation of the control.
3. *Evaluated the design and operation of control(s) and performed substantive procedures.* If the audited provider has a control or set of controls that closely aligns with some, but not all, of the criteria of the relevant DSA Specified Requirements, we executed procedures to assess the design and operation of the control for those criteria aligned with a control or set of controls and performed substantive procedures for the remaining attributes of the relevant DSA Specified Requirements.
4. *Performed substantive procedures.* If the audited provider does not have a control or set of controls that closely aligns with many aspects of the relevant DSA Specified Requirements, we solely executed substantive procedures.

The nature of our procedures to obtain evidence can include a combination of the following techniques to obtain reasonable assurance:

- (a) Inquiry – Seeking information from knowledgeable people, throughout or outside the audited provider
- (b) Observation – Watching processes or procedures being performed by audited provider personnel
- (c) Inspection – Examining records or documents
- (d) Reperformance - Independent execution, by the auditing organization, of controls or procedures originally performed by the audited provider

The timing and extent of our procedures to be performed is a matter of professional judgment and will vary based on engagement circumstances, including the materiality, subjectivity and complexity of the obligations and our risk assessment conclusions.



## Impact of notable changes to the systems and functionalities audited during the examination period

We inquired as to any notable changes made to the systems and functionalities during the DSA Examination Period and adjusted our examination procedures appropriately. To the extent the changes were deemed to have a significant impact on achieving compliance with the given DSA Specified Requirements, we denoted the nature of the change in the description of the procedures performed in Appendix 1.

## Evaluation and use of audited provider's legal interpretation, operational benchmarks and definitions

Many of the obligations needed to be supplemented by the audited provider's own legal determination, operational benchmarks and/or definition of ambiguous terms ("audited provider's developed supplemental criteria"). For each obligation, we took one of the following approaches:

1. We assessed the audited provider's developed supplemental criteria and deemed it reasonable without further expansion or adjustment. As such, we performed procedures to evaluate the audited service's compliance with the DSA Specified Requirements, including the audited provider's supplemental developed criteria.
2. We assessed the audited provider's developed supplemental criteria and deemed it reasonable but identified recommendations to improve the audited provider's developed supplemental criteria. As such, we performed procedures to evaluate the audited service's compliance with the DSA Specified Requirements, including the audited provider's supplemental developed criteria, and provided a recommendation to improve the audited provider's supplemental developed criteria.
3. We assessed the audited provider's developed supplemental criteria (if any) and deemed it insufficient to obtain reasonable assurance. In these situations, we either concluded the obligation was not met or determined we did not have sufficient criteria to conclude on the obligation.

The professional standards applied prohibit the auditing organization from developing its own criteria.

Certain audited provider's developed supplemental criteria are included within the audit criteria in Appendix 1 for each obligation that the auditing organization deemed necessary to provide for the Specified Parties to evaluate compliance and for the DSA Specified Requirements to meet the applicable professional standard's definition of suitability.

## Use of Sampling

As noted in the Delegated Regulation, the auditing organization is permitted to use sampling in the collection of audit evidence. The sample size and methodology for sampling were selected in a way to obtain representativeness of the data or information and, as appropriate, in consideration of the following:

- (a) evidence obtained throughout the DSA Examination Period, or subset of the DSA Examination Period (as appropriate);
- (b) relevant changes to the audited service during the DSA Examination Period;
- (c) relevant changes to the context in which the audited service is provided during the DSA Examination Period;
- (d) relevant features of algorithmic systems, where applicable, including personalization based on profiling or other criteria;
- (e) other relevant characteristics or partitions of the data, information and evidence under consideration;
- (f) the representation and appropriate analysis of concerns related to particular groups as appropriate, such as minors or vulnerable groups and minorities, in relation to the audited obligation, as deemed necessary.

As part of our risk assessment, we determined our preliminary audit strategy (i.e., controls reliance, substantive only strategy or combination of the two) for each individual obligation. When taking a controls reliance strategy and our procedures include obtaining evidence from multiple controls and/or additional assurance from substantive procedures,





we have selected sample sizes based on the size of the population (e.g., 10% of the population size, with a maximum sample of 25 when the population is greater than 250 occurrences and a minimum sample of 5 when the population is less than 50 occurrences).

#### *Sampling related to controls/compliance*

Based on the nature of the engagement, our procedures relate to testing compliance and/or internal control over compliance – with certain requirements. Accordingly, our testing procedures include attribute sampling to determine if the sample selected has the desired attribute (for example, the selected sample's attribute is correct or incorrect, present or absent, valid or not valid) to conclude on compliance with the DSA Specified Requirements. As such, we applied guidance for minimum sample sizes in accordance with attribute sampling techniques (i.e., a qualitative statistical sample). Due to the nature of compliance/control sampling, other traditional sampling approaches for testing are not applicable as the populations do not have quantitative dimensions (e.g., monetary balances in a financial statement audit).

#### *Sampling related to substantive procedures and other considerations for controls testing*

When we have taken a substantive only strategy or we have only identified one control to test related to the obligation, we have either (1) expanded our sample sizes (e.g., to 60) or (2) performed additional procedures to obtain sufficient evidence to conclude on the Company's compliance with the DSA Specified Requirements. These additional procedures may include obtaining specific representations from management, performing substantive analytical procedures or testing more key items.

#### *Identified exceptions in sample populations*

In all instances, when we encountered one exception within our sample selections which we determined to be random, we selected additional items for testing (e.g., for sample sizes of 25, we tested at least 15 additional items or 40 in total). When we concluded that the exception is systematic, we did not extend our sample size but instead concluded that the exception was an instance of non-compliance.



## Appendix 3 — Annex I of the Delegated Regulation — Template for the audit report referred to in Article 6 of Delegated Regulation

### Section A: General Information

<b>1. Audited service:</b>	
Google Search	
<b>2. Audited provider:</b>	
Google Ireland Limited ("GIL")	
<b>3. Address of the audited provider:</b>	
Gordon House Barrow Street Dublin 4, D04E5W5 Ireland	
<b>4. Point of contact of the audited provider:</b>	
[CONFIDENTIAL]*	
<b>5. Scope of the audit:</b>	
Does the audit report include an assessment of compliance with all the obligations and commitments referred to in Article 37(1) of Regulation (EU) 2022/2065 applicable to the audited provider?	Yes. The audit report includes assessment of compliance with Article 37(1)(a). Refer to the applicable obligations in Appendix 1. Article 37(1)(b) was not subject to audit because the requirement for the audited service to comply with such articles did not exist during the DSA Examination Period.
<b>i. Compliance with Regulation (EU) 2022/2065</b>	
Obligations set out in Chapter III of Regulation (EU) 2022/2065:	
<b>Audited obligation</b>	<b>Period covered</b>
A listing of the audited obligations can be found in Appendix 1 of our attached Assurance Report of Independent Accountants regarding the Digital Services Act.	1 June 2024 through 31 May 2025
<b>ii. Compliance with codes of conduct and crisis protocols</b>	
Commitments undertaken pursuant to codes of conduct referred to in Articles 45 and 46 of Regulation (EU) 2022/2065 and crisis protocols referred to in Article 48 of Regulation (EU) 2022/2065:	
<b>Audited commitment</b>	<b>Period covered</b>
Not applicable	Not applicable
<b>6. a. Audit start date:</b>	<b>b. Audit end date:</b>
Not applicable	Not applicable

### Section B: Auditing organisation(s)

To complete the section below, insert as many lines as necessary per point.

<b>1. Name(s) of organisation(s) constituting the auditing organisation:</b>
Ernst & Young LLP, a Delaware limited liability partnership ("EY")

\*Non-Confidential Summary of Redacted Content: personal data.



## 2. Information about the auditing team of the auditing organisation:

For each member of the auditing team, provide:

- Their personal name.
- The individual organisation, part of the auditing organisation, they are affiliated with;
- Their professional email address.
- Descriptions of their responsibilities and the work they undertook during the audit

[CONFIDENTIAL]\* was the overall responsible person from EY. (Contact detail: [CONFIDENTIAL]\*) EY has maintained a list of the engagement team members. At EY's request, for privacy purposes, the personal names are not being specified in this submission. However, the complete list of team members may be requested if required.

## 3. Auditors' qualification:

- a. Overview of the professional qualifications of the individuals who performed the audit, including domains of expertise, certifications, as applicable:

There were more than 70 university-degreed team members involved in the execution of the engagement. Personnel directing the assurance engagement collectively have significant experience related to auditing the technology industry, algorithm systems, performing risk assessment, assessing compliance functions, content moderation, privacy matters, GDPR and other related topics.

The team included individuals with the following credentials:

- Licensed Certified Public Accountant ("CPA")
  - Chartered Accountant
- Certified Information Systems Auditor ("CISA") as recognized by the Information Systems Audit and Control Association
- Certified Information Privacy Professional/United States ("CIPP/US")
- Certified Information Systems Security Professional ("CISSP") as recognized by the International Information System Security Certification Consortium, also known as ("ISC")
- Certified in Risk and Information Systems Control ("CRISC") as recognized by the Information Systems Audit and Control Association ("ISACA")
  - Admission to Practice Law as issued by various US State Bar Associations
  - ISO 27001 Auditor
  - ISO 27001 Lead Implementer - Information Security Certification
  - ISO 27001 Lead Auditor – Information Security Certification
- Prince2 Certification
- Certified Scrum Master (CSM)
- Certified Internal Auditor (CIA)

- b. Documents attesting that the auditing organisation fulfils the requirements laid down in Article 37(3), point (b) of Regulation (EU) 2022/2065 have been attached as an annex to this report:

Response included in Appendix 6.

## 4. Auditors' independence:

### a. Declaration of interests

EY performs audits, reasonable and limited assurance engagements, and related permissible professional services, for Alphabet, Inc. and GIL in our capacity as an assurance, tax, transaction, and advisory services provider. Additionally, EY performs audits, reasonable and limited assurance engagements, and related permissible professional services, for Alphabet Inc., including many of its subsidiaries, in our capacity as a global assurance, tax, transaction, and advisory services provider.

\*Non-Confidential Summary of Redacted Content: personal data.



EY has contracts to purchase certain Google services (including advertising). Google has informed us the contracts are in the ordinary course of business and the terms and conditions are “at market”, as compared to other buyers at similar levels of spending. We have concluded there is no effect on EY’s independence with respect to these contracts. In reaching that conclusion, we considered the AICPA (American Institute of Certified Public Accountants) Independence rules applicable to this situation, which permit business relationships between an audit client and the firm or covered person in the firm when the firm or covered person is a consumer in the ordinary course of business.

**b. References to any standards relevant for the auditing team’s independence that the auditing organisation(s) adheres to:**

Refer to the Assurance Report of Independent Accountants regarding the Digital Services Act. As noted in the Assurance Report of Independent Accountants, EY applies the AICPA Code of Conduct which is equivalent to (or exceeds) the International Ethics Standards Board for Accountants International Code of Ethics for Professional Accountants (including International Independence Standards), which includes independence and other requirements founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behavior. Independence is comprised of independence of mind and independence in appearance, both of which are required of the engagement team members engaged in providing reasonable assurance engagements. Independence of mind requires that the members maintain a state of mind that permits the expression of a conclusion without being affected by influences that compromise professional judgment, thereby allowing an individual to act with integrity and exercise objectivity and skepticism. Independence of appearance is achieved by the avoidance of facts and circumstances that are so significant that a reasonable and informed third party would likely conclude, weighing all the specific facts and circumstances, that a firm’s, or a member of the audit team’s, integrity, objectivity, or professional skepticism has been compromised.

**c. List of documents attesting that the auditing organisation complies with the obligations laid down in Article 37(3), points (a) and (c) of Regulation (EU) 2022/2065 attached as annexes to this report. Attachment 3 and 5 to Annex 1**

Refer to Appendix 6 which addresses Article 37(3), points (a) and (c).

**5. References to any auditing standards applied in the audit, as applicable:**

Refer to our attached Assurance Report of Independent Accountants regarding the Digital Services Act. As noted in the Assurance Report of Independent Accountants, our engagement was conducted in accordance with ISAE 3000 (revised) and attestation standards established by the AICPA. Those standards require that we plan and perform the reasonable assurance engagement to obtain reasonable assurance about whether management’s assertion is appropriately stated, in all material respects.

**6. References to any quality management standards the auditing organisation adheres to, as applicable:**

EY applies the International Standard on Quality Management I (ISQM 1) and the AICPA’s Quality Management Standard. Accordingly, we maintain a comprehensive system of quality management including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

Furthermore, EY is a registered audit firm with the Public Company Accounting Oversight Board (“PCAOB”) of the United States and is an AICPA member firm. As such, EY complies with the public accounting profession’s technical and ethical standards, including the AICPA’s Code of Professional Conduct. In addition to the Code of Professional Conduct, the AICPA publishes standards, which delineate specific requirements that Certified Public Accountants are consistently required to follow during the audit. Refer to EY Transparency Report 2024 for further background.

*Section C: Summary of the main findings*

**1. Summary of the main findings drawn from the audit (pursuant to paragraph 37(4), point (e) of Regulation (EU) 2022/2065)**

A description of the main findings drawn from the audit can be found in Appendix 1 of our attached Assurance Report of Independent Accountants regarding the Digital Services Act.



### Section C.1: Compliance with Regulation (EU) 2022/2065

- 1) Audit opinion for compliance with the audited obligations referred to in Article 37(1), point (a) of Regulation (EU) 2022/2065:

The aggregate audit opinion for compliance with the applicable audited obligations set out in Chapter III of Regulation (EU) 2022/2065 can be found within our attached Assurance Report of Independent Accountants regarding the Digital Services Act.

- 2) Audit conclusion for each audited obligation:

The audit conclusion for each audited obligation can be found in Appendix 1 of our attached Assurance Report of Independent Accountants regarding the Digital Services Act.

### Section C.2: Compliance with voluntary commitments in codes of conduct and crisis protocols

Repeat section C.2 for each audited code of conduct and crisis protocol referred to in Article 37(1), point (b) of Regulation (EU) 2022/2065:

- 1) Audit opinion for compliance with the commitments made under specify the code of conduct or crisis protocol covered by the audit:

Not applicable

- 2) Audit conclusion for each audited commitment:

Not applicable

### Section C.3: Where applicable, explanations of the circumstances and the reasons why an audit opinion could not be expressed:

Not applicable

## Section D: Description of the findings: compliance with Regulation (EU) 2022/2065

### Section D.1: Audit conclusion for obligation (specify)

#### I. Audit conclusion:

- **Description of the audit conclusion, justification, and remarks.**
- **As appropriate, include here any comments.**

A description of the audit conclusion, justification, and remarks for each audited obligation can be found in Appendix 1 of our attached Assurance Report of Independent Accountants regarding the Digital Services Act.

*If the conclusion is not 'positive', operational recommendations on specific measures to achieve compliance. Explanation on the materiality of non-compliance, where applicable*

*Recommended timeframe to achieve compliance*

Operational recommendations on specific measures to either a) achieve compliance (where the conclusion is negative), including an explanation on the materiality of non-compliance and recommended timeframe to achieve compliance, or b) improve that do not have a substantive effect on compliance (where the conclusion is positive with comments), can be found in Appendix 1 of our attached Assurance Report of Independent Accountants regarding the Digital Services Act.

#### II. Audit procedures and their results:

- 1) **Description of the audit criteria and materiality threshold used by the auditing organisation pursuant to Article 10(2), point (a) of this Regulation:**

A description of the audit criteria and materiality thresholds used can be found in Appendix 1 of our attached Assurance Report of Independent Accountants regarding the Digital Services Act.

- 2) **Audit procedures, methodologies, and results:**

- a) **Description of the audit procedures performed by the auditing organisation, the methodologies used to assess compliance, and justification of the choice of those procedures and methodologies (including,**



**where applicable, a justification for the choices of standards, benchmarks, sample size(s) and sampling method(s)):**

A description of the audit procedures performed, the methodologies used to assess compliance, and a justification of the choice of those procedures and methodologies can be found in Appendix 1 and Appendix 2 of our attached Assurance Report of Independent Accountants regarding the Digital Services Act.

**b) Description, explanation, and justification of any changes to the audit procedures during the audit:**

A description, explanation, and justification of any changes to the audit procedures during the audit can be found in Appendix 1 and Appendix 2 of our attached Assurance Report of Independent Accountants regarding the Digital Services Act.

**c) Results of the audit procedures, including any test and substantive analytical procedures:**

The results of the audit procedures, including any test and substantive analytical procedures, can be found in Appendix 1 of our attached Assurance Report of Independent Accountants regarding the Digital Services Act.

**3) Overview and description of information relied upon as audit evidence, including, as applicable:**

- a. Description of the type of information and its source;
- b. The period(s) when the evidence was collected;
- c. The period the evidence refers to;
- d. Any other relevant information and metadata.

An overview and description of information relied upon as audit evidence can be found in Appendix 1 of our attached Assurance Report of Independent Accountants regarding the Digital Services Act and Appendix 2.

**4) Explanation of how the reasonable level of assurance was achieved:**

An explanation of how the reasonable level of assurance was achieved can be found in Appendix 1 of our attached Assurance Report of Independent Accountants regarding the Digital Services Act.

**5) In cases when:**

- a. A specific element could not be audited, as referred to in Article 37(5) of Regulation (EU) 2022/2065, or
- b. an audit conclusion could not be reached with a reasonable level of assurance, as referred to in Article 8(8) of this Regulation, provide an explanation of the circumstances and the reasons:

Not applicable

**6) Notable changes to the systems and functionalities audited during the audited period and explanation of how these changes were taken into account in the performance of the audit.**

A list of notable changes to the systems and functionalities audited during the audited period and explanation of how these changes were taken into account in the performance of the audit can be found in Appendix 1 of our attached Assurance Report of Independent Accountants regarding the Digital Services Act and Appendix 2.

**7) Other relevant observations and findings:**

Please see Appendix 1 of our attached Assurance Report of Independent Accountants regarding the Digital Services Act and Appendix 2 for any other relevant observations and findings.

## Section D.2: Additional elements pursuant to Article 16 of this Regulation

**1) An analysis of the compliance of the audited provider with Article 37(2) of Regulation (EU) 2022/2065 with respect to the current audit:**

An analysis of the compliance of the audited provider with Article 37(2) of Regulation (EU) 2022/2065 with respect to the current audit can be found in Appendix 1 of our attached Assurance Report of Independent Accountants regarding the Digital Services Act.

**2) Description of how the auditing organisation ensured its objectivity in the situation described in Article 16(3) of this Regulation:**

As noted in the Assurance Report of Independent Accountants, our engagement was conducted in accordance with ISAE 3000 (revised) and attestation standards established by the AICPA. The AICPA's Code of Professional Conduct mandates that we must maintain objectivity and integrity when providing professional services and be



independent in fact and in appearance. This means we should not allow bias, conflicts of interest, or the influence of others to override our professional judgment. Accordingly, as part of engagement acceptance, we assess our independence, and throughout the engagement, we evaluate evidence to determine that it is sufficient and appropriate, by measuring the quality of the evidence (i.e., its relevance and reliability).

*Section E: Description of the findings concerning compliance with codes of conduct and crisis protocol*

*N/A – No codes of conduct and crisis protocols were applicable during the audit period.*

**Code of conduct or crisis protocol: (specify)**

Repeat this section for each code of conduct and crisis protocol.

Section E.1: Audit conclusion for commitment (specify)	
<b>I. Audit conclusion:</b>	
Description of the audit conclusion, justification, and any comments.	
<i>If the conclusion is not 'positive', operational recommendations on specific measures to achieve compliance.</i> <i>Explanation on the materiality of non-compliance, where applicable</i>	<i>Recommended timeframe to achieve compliance</i>
<b>II. Audit procedures and their results:</b>	
1. Description of the audit criteria and materiality threshold used by the auditing organisation pursuant to Article 10(2), point (a) of this Regulation:	
2. Audit procedures, methodologies, and results: a) Description of the audit procedures performed by the auditing organisation, the methodologies used to assess compliance, and justification of the choice of those procedures and methodologies (including, where applicable, a justification for the choices of standards, benchmarks, sample size(s) and sampling method(s)); b) Description, explanation, and justification of any changes to the audit procedures during the audit; c) Results of the audit procedures, including any test and substantive analytical procedures:	
3. Overview and description of information relied upon as audit evidence, including, as applicable: a) description of the type of information and its source; b) the period(s) when the evidence was collected; c) the period to which the evidence refers; d) any other relevant information and metadata.	
4. Explanation of how the reasonable level of assurance was achieved:	
5. In cases when: a. a specific element could not be audited, as referred to in Article 37(5) of Regulation (EU) 2022/2065, or b. an audit conclusion could not be reached with a reasonable level of assurance, as referred to in Article 8(8) of this Regulation, provide an explanation of the circumstances and the reasons:	





Obligation or commitment and relevant elements not audited	Explanation of circumstances and reasons:
6. Notable changes to the systems and functionalities audited during the audited period and explanation of how these changes were taken into account in the performance of the audit.	
7. Other relevant observations and findings	

### Section F: Third-parties consulted

Repeat this section per third-party consulted, incrementing the name of the section by one (for example, F.1, F.2, and so forth).

<b>1. Name of third party consulted:</b>
N/A
<b>2. Representative and contact information of consulted third party:</b>
N/A
<b>3. Date(s) of consultation:</b>
N/A
<b>4. Input provided by third-party</b>
N/A

Section G: Any other information the auditing body wishes to include in the audit report (such as a description of possible inherent limitations).

Please refer to our attached [Assurance Report of Independent Accountants regarding the Digital Services Act](#) for additional information.

		<i>Include as many lines as necessary in accordance with the allocation of responsibilities and empowerment as referred to in Article 7(1) point b)</i>	
<b>Date</b>	27 August 2025	<b>Signed by</b>	[CONFIDENTIAL]*
<b>Place</b>	303 S Almaden Blvd, San Jose, California 95110 United States	<b>In the name of</b>	Ernst & Young LLP
		<b>Responsible for:</b>	Entire Engagement

\*Non-Confidential Summary of Redacted Content: personal data.





## **Appendix 4 — Written agreement(s) between audited provider and the auditing organization**

Find the Engagement Agreement in the attached files of this document.

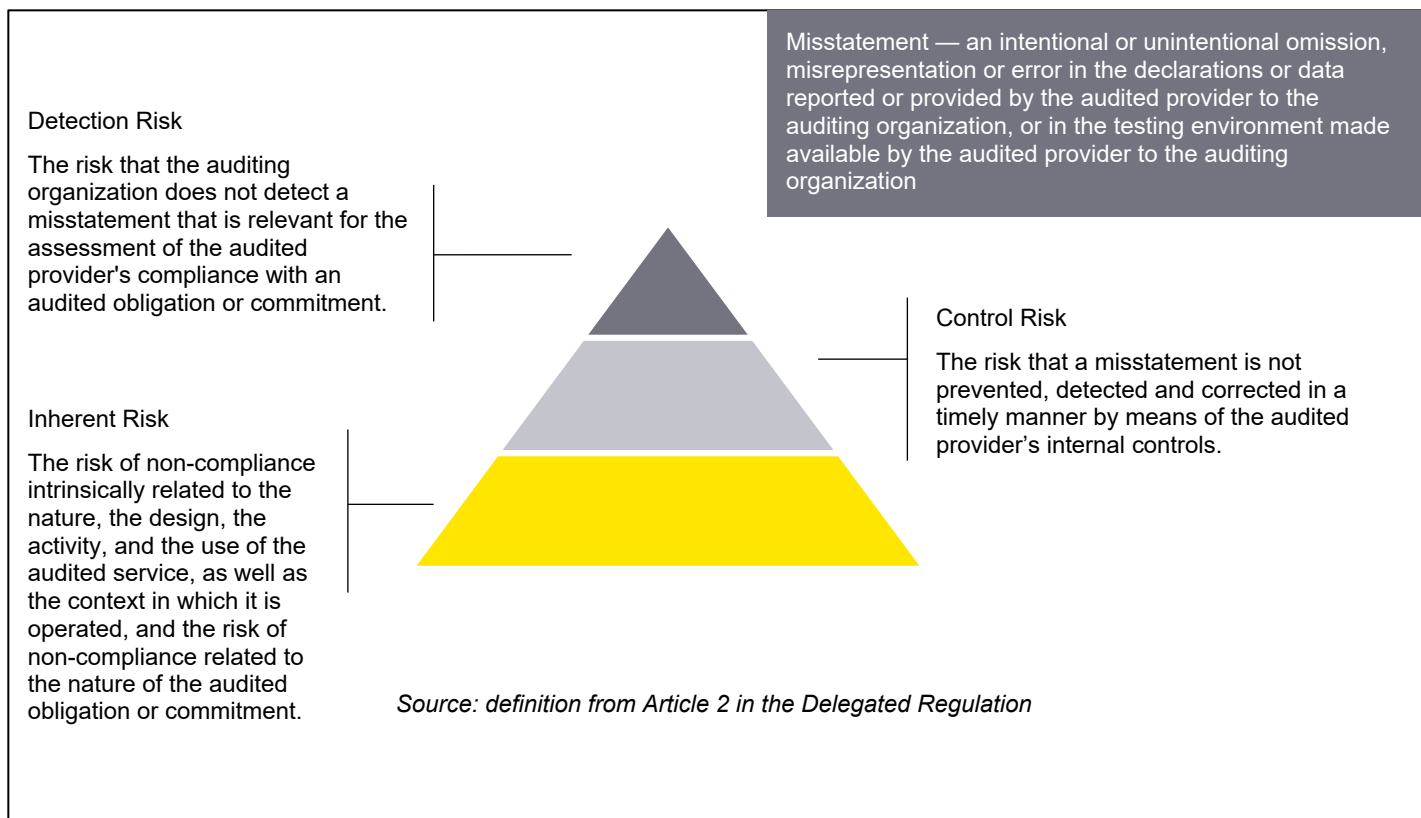


## Appendix 5 — Documents relating to the audit risk analysis

**Purpose:** This document summarizes the risk assessment performed for the assessment of compliance with each audited obligation, including the assessment of inherent risks, control risks and detection risks for each audited obligation (i.e., each sub article of the Digital Service Act).

### DSA Risk Assessment Requirements

- 1) The audit report shall include a substantiated audit risk analysis performed by the auditing organization for the assessment of the audited provider's compliance with each audited obligation.
- 2) The audit risk analysis shall be carried out prior to the performance of audit procedures and shall be updated during the performance of the audit, in the light of any new audit evidence which, according to the professional judgement of the auditing organization, materially modifies the assessment of the audit risk.
- 3) The audit risk analysis shall consider:
  - a. Inherent risks;
  - b. Control risks;
  - c. Detection risks.





4) The audit risk analysis shall be conducted considering:

- a. The nature of the audited service and the societal and economic context in which the audited service is operated, including probability and severity of exposure to crisis situations and unexpected events;
- b. The nature of the obligations;
- c. Other appropriate information, including:
  - Where applicable, information from previous audits to which the audited service was subjected;
  - Where applicable, information from reports issued by the European Board for Digital Services or guidance from the Commission, including guidelines issued pursuant to Article 35(2) and (3) of the DSA, and any other relevant guidance issued by the Commission with respect to the application of the DSA;
  - Where applicable, information from audit reports published pursuant to Article 42(4) of the DSA by other providers of very large online platforms or of very large online search engines operating in similar conditions or providing similar services to the audited service.

## Overview

Risk assessment procedures were performed to help identify risks of material misstatement and plan out the nature, timing, and extent of our audit procedures.

### Risk Assessment Steps performed:

1. We obtained an understanding of the systems and processes (and related controls) put in place to comply with the DSA Specified Requirements and other engagement circumstances.

Understanding the subject matter is key to planning and executing an effective engagement. We obtain our understanding during planning and update it throughout the performance of the engagement to the extent that changes affect our overall engagement strategy or the nature, timing, and extent of our procedures.

### We obtained an understanding sufficient to:

- Enable us to identify and assess the risks of material misstatement.
- Provide a basis for designing and performing procedures to respond to the assessed risks and to obtain reasonable assurance to support our opinion.

Information obtained to inform the audit risk analysis:

Described in Article 9 of the Delegated Regulation	Information obtained, included, but not limited to:
The nature of the audited service and the societal and economic context in which the audited service is operated, including probability and severity of exposure to crisis situations and unexpected events.	Information from audited provider (website, voice-over, annual report, trust, and safety reports) The transparency reports Systemic Risk Assessment
The nature of the obligations and commitments in Chapter 3 of the DSA	Any documentation by the audited provider concerning the scope The audited provider's risk assessment per article, including flowcharts The audit risk and control framework
Other appropriate information, including, where applicable, information from previous audits to which the audited service was subjected;	Requests for Information (RFIs) and the responses to the RFIs Internal audit reports concerning the DSA or covering topics in the DSA (e.g., content moderation).



Described in Article 9 of the Delegated Regulation	Information obtained, included, but not limited to:
	European Commission's supervision actions taken of the other designated very large online platforms and search engines under DSA
Other appropriate information, including, where applicable, information from reports issued by the European Board for Digital Services or guidance from the Commission, including guidelines issued pursuant to Article 35(2) and (3) of the DSA, and any other relevant guidance issued by the Commission with respect to the application of the DSA;	None Identified
Other appropriate information, including, where applicable, information from audit reports published pursuant to Article 42(4) of the DSA by other providers of very large online platforms or of very large online search engines operating in similar conditions or providing similar services to the audited service.	Certain published reports from other providers operating in similar conditions or providing similar services (e.g., published transparency reports, DSA audit reports, etc.)

2. We determined whether the risk factors we identify are inherent risks that may give rise to risks of material misstatement associated with the subject matter. We obtained an understanding by performing procedures, including reviews of relevant information, inquiries, data analytics, observations, and inspections.

We obtained an understanding of how management prepares certain information, such as their risk assessment to comply with Article 34. We also obtain an understanding of management's process for determining the risks that would prevent the DSA Specified Requirements from being achieved, and for designing and implementing processes and controls to address those risks. The audited provider has a formal risk assessment process to comply with Article 34, and other requirements.

We obtained an understanding of the components of the system of internal control at the entity level is an important step in performing our risk assessment procedures, as it helped us identify events and conditions that may have a pervasive effect on the susceptibility of the subject matters of our report to misstatement, either due to fraud or error. We obtained an understanding of how the audited service's system of internal control operates at the entity level, including:

- Control environment
- Monitoring activities
- Management's risk assessment process

3. For each obligation, we assessed inherent, control and detection risks.

See below for the determination of inherent, control and detection risks.

#### 4. Revision of Risk Assessment

In some instances, our assessment of the risks of material misstatement changed during the engagement as additional evidence is obtained. In circumstances in which we obtained evidence from performing further procedures, or when new information is obtained, either of which is inconsistent with the evidence on which we originally based the assessment, we revised the assessment and modified the planned procedures accordingly.



## Determination of inherent, control and detection risks for each obligation

### Overview of Risk assessment

Assessment of Risk regarding the Digital Services Act				
Obligation	Inherent Risk	Control Risk	Control Strategy	Detection Risk
11.1	Low	High	Not Rely on Controls <sup>2</sup>	Moderate
11.2	Low	High	Not Rely on Controls <sup>2</sup>	Moderate
11.3	Low	High	Not Rely on Controls <sup>2</sup>	Moderate
12.1	Low	High	Not Rely on Controls <sup>2</sup>	Moderate
12.2	Low	High	Not Rely on Controls <sup>2</sup>	Moderate
14.1	Low	High	Not Rely on Controls <sup>2</sup>	Moderate
14.2	Low	High	Not Rely on Controls <sup>1</sup>	Moderate
14.4	High	High	Not Rely on Controls <sup>1</sup>	Low
14.5	Low	High	Not Rely on Controls <sup>1</sup>	Moderate
14.6	Low	High	Not Rely on Controls <sup>1</sup>	Moderate
15.1	High	High	Not Rely on Controls <sup>1</sup>	Low
24.2	Low	High	Not Rely on Controls <sup>1</sup>	Moderate
24.3	Low	High	Not Rely on Controls <sup>1</sup>	Moderate
34.1	High	High	Not Rely on Controls <sup>1</sup>	Low
34.2	High	High	Not Rely on Controls <sup>1</sup>	Low
34.3	Low	High	Not Rely on Controls <sup>1</sup>	Moderate
35.1	High	High	Not Rely on Controls <sup>1</sup>	Low
36.1	High	High	Not Rely on Controls <sup>2</sup>	Low
37.1	Low	High	Not Rely on Controls <sup>2</sup>	Moderate
37.2	Low	High	Not Rely on Controls <sup>2</sup>	Moderate
37.3	Low	High	Not Rely on Controls <sup>2</sup>	Moderate
37.4	Low	High	Not Rely on Controls <sup>2</sup>	Moderate
37.5	Low	High	Not Rely on Controls <sup>2</sup>	Moderate
37.6	Low	High	Not Rely on Controls <sup>2</sup>	Moderate
38	High	High	Not Rely on Controls <sup>1</sup>	Low
39.1	High	High	Not Rely on Controls <sup>1</sup>	Low
39.2	High	Low	Rely on Controls	High
39.3	High	Low	Rely on Controls	High
40.1	Low	High	Not Rely on Controls <sup>1</sup>	Moderate
40.12	Low	High	Not Rely on Controls <sup>1</sup>	Moderate
41.1	Low	High	Not Rely on Controls <sup>2</sup>	Moderate
41.2	Low	High	Not Rely on Controls <sup>2</sup>	Moderate



Assessment of Risk regarding the Digital Services Act				
Obligation	Inherent Risk	Control Risk	Control Strategy	Detection Risk
41.3	Low	High	Not Rely on Controls <sup>2</sup>	Moderate
41.4	Low	High	Not Rely on Controls <sup>2</sup>	Moderate
41.5	Low	High	Not Rely on Controls	Moderate
41.6	Low	High	Not Rely on Controls	Moderate
41.7	Low	High	Not Rely on Controls	Moderate
42.1	Low	High	Not Rely on Controls <sup>2</sup>	Moderate
42.3	Low	High	Not Rely on Controls <sup>1</sup>	Moderate
42.4	Low	High	Not Rely on Controls <sup>2</sup>	Moderate
42.5	Low	High	Not Rely on Controls	Moderate

<sup>1</sup>For certain obligations within this sub article, we have relied on controls to determine the appropriate procedures to be performed.

<sup>2</sup>For all obligations within this sub article, although the audited service has a control or set of controls that closely aligns with the Specified Requirement, we executed substantive procedures and did not perform procedures to assess the design and operation of the controls, as we deemed the substantive approach to be more efficient.



## Appendix 6 — Documents attesting that the auditing organization complies with the obligations laid down in Article 37(3), point (a), (b), and (c)

DSA Annex	Illustrative Response
Documents attesting that the auditing organisation complies with the obligations laid down in Article 37(3), point (a) of Regulation (EU) 2022/2065.	<p>We have complied with the American Institute of Certified Public Accountant's (AICPA) Code of Conduct which includes independence and other requirements founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behavior, that are at least as demanding as the applicable provisions of the International Ethics Standards Board for Accountants International Code of Ethics for Professional Accountants (including International Independence Standards).</p> <p>Our engagement agreement notes our compliance with Article 37(3)(a)(i). Since this is the second year of the DSA audit requirement, we are, by definition, in accordance with Article 37(3)(a)(ii). Regarding Article 37(3)(a)(iii), we are not performing the audit in return for fees which are contingent on the result of the audit.</p>
Documents attesting that the auditing organisation complies with the obligations laid down in Article 37(3), point (b) of Regulation (EU) 2022/2065.	<p>In compliance with Article 37(3)(b), we conclude that we have the requisite knowledge, skills, and professional diligence under the ISAE 3000 and the AICPA Attestation standards. We have applied these professional standards throughout the course of our engagement.</p>
Documents attesting that the auditing organisation complies with the obligations laid down in Article 37(3), point (c) of Regulation (EU) 2022/2065.	<p>We have complied with the AICPA Code of Professional Conduct, which includes independence and other requirements founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behavior, that are at least as demanding as the applicable provisions of the International Ethics Standards Board for Accountants International Code of Ethics for Professional Accountants (including International Independence Standards).</p> <p>We applied the International Standard on Quality Management and accordingly maintained a comprehensive system of quality management including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.</p>



## Appendix 7 — Definitions

For purposes of this assurance report the following terms have the meanings attributed below:

Term	Definition	Source
<b>Assurance engagement</b>	An engagement in which a practitioner aims to obtain sufficient appropriate evidence to express a conclusion designed to enhance the degree of confidence of the intended users other than Google Search about the subject matter information (that is, the outcome of the measurement or evaluation of an underlying subject matter against criteria).	B
<b>Audit Criteria</b>	The criteria against which the auditing organization assesses compliance with each audited obligation.	A
<b>Audit evidence</b>	Any information used by an auditing organization to support the audit findings and conclusions and to issue an audit opinion, including data collected from documents, databases or IT systems, interviews or testing performed.	A
<b>Audited obligation</b>	An obligation referred to in Article 37(1) of Regulation (EU) 2022/2065 which forms the subject matter of the audit. Unless noted otherwise, each sub article is an audited obligation.	A
<b>Auditing organization</b>	An individual organization, a consortium or other combination of organizations, including any sub-contractors, that the audited provider has contracted to perform an independent audit in accordance with Article 37 of the DSA.	A
<b>Auditing procedure</b>	Any technique applied by the auditing organization in the performance of the audit, including data collection, the choice and application of methodologies, such as tests and substantive analytical procedures, and any other action taken to collect and analyze information to collect audit evidence and formulate audit conclusions, not including the issuing of an audit opinion or of the audit report.	A
<b>Audited provider</b>	The provider of an audited service which is subject to independent audits pursuant to Article 37(1) of the DSA.	A
<b>Audit risk</b>	The risk that the auditing organization issues an incorrect audit opinion or reaches an incorrect conclusion concerning the audited provider's compliance with an audited obligation, considering detection risks, inherent risks and control risks with respect to that audited obligation.	A
<b>Audited service</b>	A very large online platform or a very large online search engine designated in accordance with Article 33 of the DSA.	A
<b>Control risk</b>	The risk that a misstatement is not prevented, detected and corrected in a timely manner by means of the audited provider's internal controls.	A
<b>Criteria</b>	The benchmarks used to measure or evaluate the underlying subject matter.	B
<b>Detection risk</b>	The risk that the auditing organization does not detect a misstatement that is relevant for the assessment of the audited provider's compliance with an audited obligation.	A
<b>Engagement risk</b>	The risk that the practitioner expresses an inappropriate conclusion when the subject matter information is materially misstated.	B
<b>Evidence</b>	Information used by the practitioner in arriving at the practitioner's conclusion. Evidence includes both information contained in relevant information systems, if any, and other information.	B





Term	Definition	Source
<b>Inherent risk</b>	The risk of non-compliance intrinsically related to the nature, the design, the activity and the use of the audited service, as well as the context in which it is operated, and the risk of non-compliance related to the nature of the audited obligation.	A
<b>Intended users</b>	The individual(s) or organization(s), or group(s) thereof that the practitioner expects will use the assurance report.	B
<b>Internal control</b>	Any measures, including processes and tests, that are designed, implemented and maintained by the audited provider, including its compliance officers and management body, to monitor and ensure the audited provider's compliance with the audited obligation.	A
<b>Materiality threshold</b>	The threshold beyond which deviations or misstatements by the audited provider, individually or aggregated, would reasonably affect the audit findings, conclusions and opinions.	A
<b>Misstatement</b>	A difference between the subject matter information and the appropriate measurement or evaluation of the underlying subject matter in accordance with the criteria. Misstatements can be intentional or unintentional, qualitative or quantitative, and include omissions.	B
<b>Practitioner</b>	The individual(s) conducting the engagement (usually the engagement partner or other members of the engagement team, or, as applicable, the firm).	B
<b>Professional judgment</b>	The application of relevant training, knowledge, and experience, within the context provided by assurance and ethical standards, in making informed decisions about the courses of action that are appropriate in the circumstances of the engagement.	B
<b>Professional skepticism</b>	An attitude that includes a questioning mind, being alert to conditions which may indicate possible misstatement, and a critical assessment of evidence.	B
<b>Reasonable assurance engagement</b>	An assurance engagement in which the practitioner reduces engagement risk to an acceptably low level in the circumstances of the engagement as the basis for the practitioner's conclusion. The practitioner's conclusion is expressed in a form that conveys the practitioner's opinion on the outcome of the measurement or evaluation of the underlying subject matter against criteria.	B
<b>Subject matter</b>	The phenomenon that is measured or evaluated by applying criteria.	B
<b>Subject matter information</b>	The outcome of the measurement or evaluation of the underlying subject matter against the criteria, i.e., the information that results from applying the criteria to the underlying subject matter.	B
<b>Substantive analytical procedure</b>	An audit methodology used by the auditing organization to assess information to infer audit risks or compliance with the audited obligation.	A
<b>Test</b>	An audit methodology consisting in measurements, experiments or other checks, including checks of algorithmic systems, through which the auditing organization assesses the audited provider's compliance with the audited obligation.	A
<b>Vetted researcher</b>	A researcher vetted in accordance with Article 40(8) of the DSA.	A

Sources used:

A – Delegated Regulation Article 2

B - ISAE 3000 (Revised), *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*



Ernst & Young LLP  
303 Almaden Boulevard  
San Jose, California

Tel: +1 408 957 5500  
ey.com

Google Ireland Limited  
Gordon House  
Barrow Street  
Dublin 4 D04 E5W5  
Ireland

This Services Agreement (“**Agreement**”) is entered into between **Ernst & Young LLP**, a Delaware limited liability partnership (“**EY**”) and **Google Ireland Limited** (“**GIL**,” “**Google**,” or “**Client**”) effective as of the date of last signature (the “**Effective Date**”), and incorporates the General Terms and Conditions attached hereto as Appendix 1 (together, this “**Contract**”).

## Scope of Services

1. Within the European Union, GIL is the sole service provider of each of the services, **Google Play**, **Google Maps**, **Google Shopping**, **YouTube**, and **Google Search**, (each, an “**audited service**”) designated as Very Large Online Platforms (“**VLOPs**”) / Very Large Online Search Engines (“**VLOSE**”) by the European Commission, under Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 ( the “**Digital Services Act**” or “**DSA**” or “**Act**”).
2. **Subject Matter.** EY will:
  - 2.1. examine the Client’s assertion that the processes and controls implemented for each of the services designated as VLOPs/VLOSE to comply with all obligations and commitments in the aggregate as well as with each applicable individual obligation and commitment referred to in Article 37 (1) of the DSA (such obligations and commitments, the “**Specified Requirements**”) during the period from 01 June 2024 through 31 May 2025 (the “**Examination Period**”); and
  - 2.2. opine on the audited service’s compliance with the Specified Requirements.

Together, the examination and opinion are referred to herein as “**the DSA Audit**” or “**Services**.” The Client agrees that only the obligations and commitments identified in this Contract are included within the scope of the DSA Audit.

3. In accordance with the Act, under Article 37 1(b), and the Delegated Regulation (including Annex I) EY will assess compliance with any commitments undertaken pursuant to the codes of conduct referred to in Articles 45 and 46 and the crisis protocols referred to in Article 48 once the Client is required to comply with such articles. Until then, EY is not expected to include any other commitments pursuant

to the previously referenced articles in EY's assessment because the Client's requirement to comply with such articles does not otherwise currently exist (i.e., the obligations do not commence until the later of the following dates: (a) the date from which the code of conduct or crisis protocol formally applies; or (b) the date from which the European Commission or the Board for Digital Services formally recognizes a code of conduct or crisis protocol as falling within the meaning of Articles 45, 46 or 48). If the European Commission takes additional action on (a) or (b) with an effective date prior to the end of the Examination Period, any inclusion of the code of conduct and crisis protocols will be as mutually agreed between the parties.

4. **Attestation Standards.** EY will conduct the DSA Audit in accordance with the attestation standards described in *International Standards on Assurance Engagements Other than Audits or Reviews of Historical Financial Information ("ISAE 3000 (Revised)")*, the attestation standards established by the American Institute of Certified Public Accountants' ("**AICPA**"), applicable aspects of the Commission Delegated Regulation supplementing Regulation (EU) 2022/2065 (the "**Delegated Regulation**"), the terms of this Agreement together with any relevant, published guidance issued by the European Commission regarding the DSA Audit.
  - 4.1. **Reasonable Assurance.** EY will plan and perform its examination to obtain reasonable assurance about whether the audited service is in compliance with the Specified Requirements, in all material respects.
  - 4.2. **Materiality.** Items are considered material, regardless of size, if they involve an omission or misstatement relevant to the audited service's compliance with the Specified Requirements that, in the light of surrounding circumstances, makes it probable that the judgment of a reasonable person relying on the information would be changed or influenced by the omission or misstatement. Concretely, this is measured in relation to whether a control was not suitably designed and operated effectively to satisfy the obligation for at least 95% of the Examination Period, and/or if there was an actual or projected error of more than 5% (or other material qualitative variance) during the Examination Period related to the audit criteria.
5. **Audit Reports.**
  - 5.1. Upon completion of the DSA Audit, EY will issue five written reports together with all their annexes in accordance with Article 37(4) of the DSA and Article 6 of the Delegated Regulations (the "**Reports**").
  - 5.2. This Contract as well as any other contracts, agreements or engagement letters between EY and the Client related to the performance of the DSA Audit, including where changes are

made to this Contract during the performance of the DSA Audit, shall be annexed to or indicated within the Report(s) per Article 7(2) and Article 7(3) of the Delegated Regulation.

### Limitations on Scope

6. **Defects or Errors in Client Systems.** EY will not identify, address or correct any errors or defects in the Client's computer systems, other devices or components thereof ("Systems"), whether or not due to imprecise or ambiguous entry, storage, interpretation or processing or reporting of data. EY will not be responsible for any defect or problem arising out of or related to data processing in any Systems.
7. **Risks of Non-Detection of Material Omissions, Misstatements, or Errors.** Because of the inherent limitations of an examination engagement, together with the inherent limitations of internal control, risk exists that some material omissions, misstatements or errors may not be detected, even though the examination is properly planned and performed in accordance with the attestation standards.
8. **Use of Reports.** Notwithstanding anything to the contrary in the General Terms and Conditions (as included at Appendix 1), the Client agrees that EY's Report(s) are intended solely for the Client's information and use, and for the information of the European Commission and the Irish Digital Services Coordinator, CnaM, mandated under DSA Article 42(4), (collectively, the "**Specified Parties**") and, unless otherwise required by law, are not intended to be, and should not be, used by anyone other than the Specified Parties unless EY has given its prior written consent. The Client acknowledges that the Report(s) will include language stating that the Report's use will be limited to the previously referenced Specified Parties.
  - 8.1. **Responsibility for Submitting Reports.** Pursuant to DSA Article 42(4), the Client will be exclusively responsible for submitting EY's Report(s) to the European Commission and the Irish Digital Services Coordinator, CnaM. The Client will also be responsible for making the Report(s) publicly available.
  - 8.2. **Disclosure of Report to Specified Parties.** The Client may disclose EY's Report(s) to the Specified Parties either:
    - 8.2.1. without EY's consent, provided that the Client discloses it in the original complete and unaltered form provided by EY; or
    - 8.2.2. with redactions by Client in accordance with DSA Article 42(5) categories, provided that Client consults with EY to confirm that such redactions do not alter the meaning of the Report or otherwise render EY out of compliance with its professional obligations; or

- 8.2.3. with redactions as agreed with EY, provided the Client agrees to provide EY with a copy of any proposed redactions to EY's Reports and the Client agrees that it shall make changes as EY may reasonably suggest in order for EY to comply with its professional obligations.

### 8.3. Further Distribution of Reports.

- 8.3.1. Subsequent to the issuance of EY's Report(s), the Client may ask EY to consider further distribution of its Report(s). If EY agrees in writing, the Client may further distribute the written Reports provided that it follows the same process as noted for the Specified Parties. Once the Reports have been made public in accordance with DSA Article 42(3)(c), the Client may refer to the Reports and distribute a public link to the Reports (as available on the Transparency Center) without EY's consent.
- 8.3.2. Additionally, the Client agrees that, without EY's prior written consent it will not, and will not permit others to, quote or refer to the Reports, any portion, summary or abstract thereof, or to EY or any other EY Firm, in any document filed or distributed in connection with (i) a purchase or sale of securities to which the United States or state securities laws ("**Securities Laws**") are applicable, or (ii) periodic reporting obligations under Securities Laws. The Client will not contend that any provisions of Securities Laws could invalidate any provision of this Agreement.

## Client's Specific Obligations

- 9. **Assertions and Selection of Specified Requirements.** The Client's management is responsible for its assertions, including selecting the applicable Specified Requirements that EY will evaluate, comprising the obligations and commitments required by the Act under Chapter III. The Client is responsible for having a reasonable basis to evaluate its compliance with the Specified Requirements, and has performed an evaluation of its compliance with the Specified Requirements. EY may assist the Client to identify additional proposed Specified Requirements for consideration, but it is the Client's choice to add any provisions to the Specified Requirements.
- 10. **Design, Implementation, and Maintenance of Internal Controls and Monitoring of Compliance.** Furthermore, the Client is responsible for:
  - 10.1. Designing, implementing, and maintaining internal controls to provide reasonable assurance that the Client complies with those Specified Requirements and
  - 10.2. Evaluating and monitoring the Client's compliance with the Specified Requirements. The Client will provide EY with a written assertion that the audited service is in compliance with

the Specified Requirements and a letter of representations at the conclusion of the engagement.

- 10.3. Providing EY with the information specified by the Digital Services Act and the Delegated Regulation (Article 5 (1)) prior to EY beginning any audit procedures. The Client is responsible for the sufficiency of the documentation of its controls for its purposes. Furthermore, the Client agrees to provide EY with the necessary evidence for EY to sufficiently comply with its responsibilities in accordance with the Delegated Regulation and professional standards.
- 10.4. Identifying and complying with all legal and other requirements applicable to the conduct of its business and other activities.
11. **Provision of EY Access.** Per Delegated Regulation Recital 12, the Client shall provide EY with access to “all information necessary for the performance of the audit,” including agreements, documents, and electronic files pertinent to the scope of this engagement. Specifically, the Client shall provide EY with the following “without undue delay in a manner that does not hamper the performance of” the DSA Audit:
  - 11.1. access to information relevant to the audited service’s systems and manual processes (and related controls) relevant to compliance with the Specified Requirements; including, per Delegated Regulation Recital 13, “personal data, collected from various sources, such as documents, algorithmic systems, databases or interviews, as appropriate.”
  - 11.2. access to procedures and processes, IT systems such as algorithmic and information systems, including testing environments, personnel and premises of that provider, and any relevant sub-contractors;
  - 11.3. access to any additional information that EY may request, as applicable;
  - 11.4. unrestricted access to persons from whom EY determines it necessary to obtain evidence;
  - 11.5. reports prepared by compliance functions (e.g. internal audit) relevant to compliance with the Specified Requirements;
  - 11.6. information that facilitates the understanding of the audited service, the Client’s’ governance, the competence of respective teams and decision-making structures, including Client’s’ compliance function, as well as presentations of Client’s information technology systems, data and records structures, and the interplay between different algorithmic systems of relevance to the audit; and
  - 11.7. assistance and explanations necessary for EY to analyze the relevant information.

12. The Client's responsibility to provide access to information set out in paragraph 11 above includes identifying the use of new technologies or techniques (e.g., the use of generative artificial intelligence) in the audited service's system and manual processes (and related controls) relevant to compliance with the Specified Requirements and in preparing information provided to EY, and additional details EY may require regarding the use of any such technologies and techniques in order to perform EY's procedures. The Client's failure to comply with this paragraph may cause EY to delay EY's Report, modify EY's procedures, or even terminate the Services.
13. To the extent the Client's internal audit team, or others performing internal control related procedures, provide direct assistance to EY in the course of the engagement, the Client agrees that they will be allowed to follow EY's instructions and Client's personnel will not intervene in the work of those individuals performing work for EY.
14. The Client shall apprise EY timely of all allegations involving improprieties that management or the Audit Committee receives (regardless of the source or form and including, without limitation, allegations by "whistle-blowers") that are relevant to the Subject Matter covered by the Services and shall provide EY with prompt and full access to these allegations and any internal investigations of them.
15. **Attorney Client Privilege:** EY acknowledges that Client does not intend for provision of any documents or information under this Agreement to be construed as a waiver, destruction, or invalidation of the attorney-client privilege, confidentiality obligations, or other legal rights, which Client and/or relevant privilege holders intend(s) to maintain, notwithstanding that EY makes no representation as to the applicability of attorney-client privilege or other legal rights over any documents or information provided by Client.
  - 15.1. If the Client limits the information otherwise available to EY (based on claims of attorney/client privilege, work product doctrine, or otherwise), the Client will immediately inform EY that certain information is being withheld. Any such withholding of information could be considered a restriction on the scope of the Services and may prevent EY from issuing its Report(s), alter the form of the Report(s) it may issue, or otherwise affect EY's ability to perform the Services. EY will disclose any such withholding of information to the Audit Committee.
16. **EY Independence.** The Client will assess and conclude prior to engaging EY that EY has fulfilled the conditions as stated in Article 37(3) of Regulation (EU) 2022/2065. EY has assessed and concluded that it has fulfilled the conditions regarding independence as stated in Article 37(3) of Regulation (EU) 2022/2065. The Client will make appropriate inquiries to determine whether the Client has a business relationship with EY or any other member firm of the global Ernst & Young organization (any

of which, an “EY Firm”). Such relationships exclude those where an EY Firm performs professional services or where an EY Firm is a consumer in the ordinary course of business. The Client will discuss with EY any matters that, in its judgment, might bear upon EY’s independence.

17. **Other Information.** Pursuant to DSA Art. 42(4), EY’s Reports are expected to be included in the Client’s submission to the European Commission (the balance of such submission, the “Other Information”). As such, the Client agrees to provide a draft of the Other Information to EY, allowing EY an opportunity to suggest modifications that may be warranted to the Other Information prior to submission. EY’s procedures will be limited to reading the Other Information for any material inconsistencies between the Other Information and EY’s Report(s) or any material misstatements of fact in the Other Information.
18. The Client shall apprise EY, in a timely manner, to the extent that Client is aware, of technical incidents and glitches, up to the date of the Report, that could have more than inconsequential impact on the Audited Services’ compliance with the Specified Requirements. A technical incident is an occurrence that actually or potentially jeopardises the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
19. **Testing Services.** The Client agrees that the Services may include automated and manual intrusive testing procedures of the Client’s or a third party’s information systems (“Testing Services”), and the Client consents to EY’s performance of such Testing Services.
20. The Client represents that, to the extent applicable, it has obtained consent from any third-party service providers as may be required in connection with the Testing Services.
  - 20.1. The Client understands that such Testing Services may result in disruptions of and/or damage to the Client’s or a third party’s information systems and/or the information and data contained therein. The Client is solely responsible for any damage caused by Testing Services and shall bring no claim against EY in connection with, or arising out of, any Testing Services, including with respect to any third-party claim against the Client related thereto, except to the extent arising out of EY’s willful misconduct. The Client and EY will seek to limit testing to non-production environments; to the extent any testing is required in a production environment, the parties will work to agree on protocols to minimize the risk of any such testing.

#### EY’s Specific Obligations



21. EY has obtained pre-concurrence from the Audit Committee related to the Services EY is to provide under this Contract.
22. As part of the Services, as noted in Paragraph 18 of the General Terms & Conditions, EY agrees that it shall take all reasonably necessary steps and security precautions in accordance with commercially reasonable industry standards to minimize the risk of unauthorized access to, or sabotage of, the Client Information and Personal Data that is provided to EY to perform the Services.
23. **Prohibition on Disclosure of Personal Data.** Given that the DSA does not change or waive existing rights and legal responsibilities relating to “[t]he protection of individuals with regard to the processing of personal data” (DSA Recital 10), consistent with Paragraphs 16-18 of the General Terms and Conditions, EY agrees that it will not, and that it will require that any agents or employees thereof who access or review any personal data on any Client services or platforms for the purposes of the DSA Audit will not, direct the disclosure of any such data for any purpose.

#### **Specific Additional Terms and Conditions**

24. For the avoidance of doubt, in performing the Services as described herein, EY and the Client agree that:
  - 24.1. The Report(s) to be issued by EY will contain relevant supporting documentation attesting that EY fulfills the necessary conditions as described in Article 37 (3) of Regulation (EU) 2022/2065 of the Digital Services Act.
  - 24.2. The audit conclusions with respect to each audited obligation and commitment, will be reported upon in accordance with Recital 16 and Article 8 of the Delegated Regulation, including being in the form of either ‘positive’, ‘positive with comments’ or ‘negative’ conclusions. For the purposes of reporting audit conclusions, EY will apply the guidance in the Delegated Regulation, including:
    - 24.2.1. Positive with comments' is used when the nature of the comments does not substantially affect the assessment of compliance itself
    - 24.2.2. Where an audit conclusion is ‘negative’ but applies only for a limited period of time and EY deems that the Client complied with the obligation or commitment for the rest of the audited period, this will be reflected in the audit Report(s) for each obligation or commitment concerned.

24.2.3. Where the audit opinion is not 'positive', provide operational recommendations on specific measures to achieve compliance and the recommended timeframe to achieve compliance

25. The Client is responsible to take due account of the operational recommendations addressed to them in a Report(s) that is not 'positive' with a view to take the necessary measures to implement them. The Client shall, within one month from receiving those recommendations, adopt an audit implementation report referred to in Article 37(6) of Regulation (EU) 2022/2065 of the Act setting out those measures. Where the Client does not implement the operational recommendations, they shall justify in the audit implementation report the reasons for not doing so and set out any alternative measures that they have taken to address any instances of non-compliance identified.
26. EY and the Client agree to use the definitions included within Article 2 of the Delegated Regulation.
27. In order to have appropriate Specified Requirements, the Client will define terms, where appropriate or necessary, in the Specified Requirements. EY may assist the Client in developing the wording of definitions included in EY's Report (if deemed necessary).
28. Although EY may review the process for making legal determinations by the Client in connection with the DSA Audit, EY will not provide legal advice, or provide opinions of legal interpretation, and any Report(s) issued by EY may not be represented as such.
29. EY makes no representations as to whether the form or content of the Report(s) to be delivered in connection with these Services satisfy the requirements of the Digital Services Act, and any interpretations or application by the European Union, European Commission or other relevant regulatory agency responsible for the monitoring or enforcement of the Digital Services Act.
30. In the course of performing the Services described in this Contract, EY and the Client may agree that certain obligations and commitments identified by the Client in relation to compliance with the Digital Services Act fall outside of the experience of EY. Where EY determines that it is not possible to address such obligations or commitments, the parties agree that these obligations or commitments will be excluded from the DSA Audit and from any Report(s) issued by EY.
31. To the extent that EY and the Client mutually agree that it is necessary to utilize a subcontractor in the performance of these Services, EY will confirm that such subcontractor individually fulfills the requirements laid down in Article 37(3), points (a) and (c), of Regulation (EU) 2022/2065 of the Act, and that all such subcontractors, jointly, fulfill the requirements laid down in Article 37(3), (b) of Regulation (EU) 2022/2065 of the Act. EY will remain liable for all subcontracted obligations and all acts or omissions of its subcontractors. EY may not subcontract any portion of its performance of the DSA Audit services without the Client's prior written consent.

32. To the extent that the Delegated Regulation is amended, or added to by the European Commission, EY and the Client agree to review and revise this Contract as may be deemed necessary.
33. The Client acknowledges that EY may be requested to make certain audit documentation available to various regulatory authorities and that nothing in this Agreement shall preclude EY from complying with such a request. Except where precluded by applicable law or regulation, EY agrees to promptly notify the Client of any such request, and if reasonably practicable, prior to any such disclosure.

## Timetable

34. The audit will be conducted on a phased basis, including (a) Planning (including execution of this Contract), (b) fieldwork and testing; and (c) reporting. Subject to the terms of this Agreement, EY will endeavour to complete and deliver the Services to the client on or before 28 August 2025.
35. In order to meet the statutory deadline for completion of the DSA Audit, the milestone delivery schedule will be as follows:

Milestone	Step	Anticipated delivery
1	Agreement signed	10 January 2025
2	Completion of Group 1 initial walkthroughs	31 January 2025
3	Completion of Group 2 initial walkthroughs	28 February 2025
4	Completion of Group 3 initial walkthroughs	31 March 2025
5	Completion of follow ups and open items relevant to initial walkthroughs	31 May 2025
6	Update testing (To complete population testing)	30 June 2025
7	Delivery of draft Reports (on a rolling basis)	from 28 July 2025
8	Delivery of final Reports	28 August 2025

36. In addition, the Client and EY will agree to a more detailed project plan, including mutually agreed turnaround times for evidence requests and evidence, and appropriate protocols for escalations (including for timeline concerns).

## Contacts/Information request process

37. The Client has identified [CONFIDENTIAL]\* as its contact with whom EY should communicate about these Services. EY will provide information, data and interview requests, including data access referred to in Article 5(2), to the designated point of contact, or others from whom EY has received requested information (e.g., follow-up requests). EY and any agents or employees thereof will provide reasonable advance notice to the Client regarding proposed scheduling of access to persons

\*Non-Confidential Summary of Redacted Content: personal data.

and documents, including walkthroughs and interviews. EY and the Client will engage in good faith consultation on scheduling EY's access to persons and documents without undue delay.

## Fees

38. The General Terms and Conditions of the Contract address EY's fees and expenses.
39. The final fee for the services will be based on the actual hours incurred using the agreed-upon rate card, in accordance with the terms of this Contract. The total aggregate invoiced amount for Services under this Agreement will not exceed the total amounts indicated below subject to discussion between Client and EY based on actual hours incurred. Please note that the 2025 fees will be based on actual effort spent for the activities to complete the DSA Audit according to the agreed upon work plan.

Table 1 –Total Fees and Expenses related to obligations as of the date of signing of this Agreement

Description	Estimated 2025 Fees
Professional Fees	[CONFIDENTIAL]*
Out-of-Pocket Expenses <sup>1</sup>	[CONFIDENTIAL]*
Total	[CONFIDENTIAL]*

- 39.1. Payment: Prior to starting work on each phase (excluding signing of the SOW which will be billed based on actuals incurred), EY and the Client will discuss the work required to align on a reasonable range of associated fees and expenses for that phase provided all requested information to make such assessment is provided to EY prior to each phase. Should there be any significant changes to the project scope or assumptions subsequent to the execution of this Agreement, EY will discuss the matter with Client, and if necessary, any such changes will be documented and agreed to in an addendum to this Agreement.

EY is in sole control of how it compensates its personnel and is solely responsible for all wage, benefit, insurance, social security, and other amounts required by law or by contract to be paid to or in respect of such personnel by his or her employer. EY warrants that it (i) will only use W-2 employees (or the local equivalent), partners, or principals of EY or an EY Firm to provide the Services, and (ii) will comply with all applicable labor or employment-related

<sup>1</sup> Actual out-of-pocket expenses will be billed as incurred.

\*Non-Confidential Summary of Redacted Content: information relating to the auditor's fees.

laws, including wage and hour and expense reimbursement laws, with respect to its personnel providing Services.

The foregoing expenses will only be reimbursed if such expenses are (i) reasonable, actual, and necessary (without mark-ups or commissions); and (ii) accompanied by such documentation, if requested by Client, establishing the type, date, amount, payment and purpose for such expense.

The parties understand and agree that nothing in this Section or the Agreement controls the reimbursements EY provides to its personnel. EY is in sole control of how it reimburses its personnel providing Services for their expenses.

- 39.2. Production and Witness Expenses: EY will provide Client with prompt notice of any requirement to produce information or personnel as witnesses with respect to which EY determines that it will seek reimbursement pursuant to Section 26 of the Agreement and will not in any event invoice Client for professional time and expenses in excess of \$1,000 without providing such notice. In the event EY provides such notice, EY will from time-to-time, as appropriate or as may reasonably be requested by Client, advise Client of the necessity of the production of such information or personnel, with respect to any such matter and, in connection therewith, provide Client with a summary of any incurred time and expenses for which EY will seek reimbursement.
- 39.3. Invoices: EY shall bill the Client for its fees and expenses and applicable taxes on a monthly basis based on actuals incurred. Payment is due 45 days from the receipt of EY's invoice. If the Client disputes any amount on an invoice, it shall promptly advise EY as to the amount in dispute and the reasons for such dispute. The parties shall cooperate diligently and in good faith to resolve any such dispute. The Client shall not withhold payment of undisputed amounts, pending resolution of any such dispute. EY will submit invoices to Client's online portal at <https://gist-uploadmyinvoice.appspot.com/>. Hard copies of the invoices do not need to be mailed to the Client once submitted to the online portal. EY must re-submit invoices if there is no receipt confirmation of the invoice submission within 24 hours. Invoices are considered received on the date of submission to the online portal so long as a receipt confirmation is received subsequent to the submission.

EY will include the relevant Client-issued P.O. numbers on all invoices submitted through the online portal. EY will re-submit invoices if there is no receipt confirmation of the invoices submission within 24 hours. EY will concurrently email a copy of the invoice to the Client's designated point of contact listed above.

In witness whereof, the parties have executed this Contract as of the date set forth above.

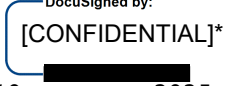
**Ernst & Young LLP**

By:  Signed by:  
[CONFIDENTIAL]\*  
09 January 2025

[CONFIDENTIAL]\*

**Partner** Audit Partner

**Google Ireland Ltd.**

Signed:  DocuSigned by:  
[CONFIDENTIAL]\*  
Date: 10 January 2025

**Authorised Signatory**

[CONFIDENTIAL]\*

Director

\*Non-Confidential Summary of Redacted Content: personal data.

## **APPENDIX I – GENERAL TERMS AND CONDITIONS**

### **Definitions**

1. The following terms are defined as specified below:

- (a) “AICPA” means the American Institute of Certified Public Accountants.
- (b) “Client Affiliate” means an entity that controls, is controlled by, or is under common control with, the Client.
- (c) “Client Entity” means the Client or a Client Affiliate.
- (d) “Client Information” means information obtained by EY from the Client or from a third party on the Client’s behalf.
- (e) “Deliverables” means any advice, communications, information, technology or other content that EY provides under this Contract.
- (f) “EY Firm” means a member of the EY network and any entity operating under a common branding arrangement with a member of the EY network.
- (g) “EY Persons” means EY’s or any other EY Firm’s subcontractors, members, shareholders, directors, officers, partners, principals or employees.
- (h) “Internal Support Services” means internal support services utilized by EY, including but not limited to:
  - (a) administrative support, (b) accounting and finance support, (c) network coordination, (d) IT functions including business applications, system management, and data security, storage and recovery, and (e) conflict checking, risk management and quality reviews.
- (i) “Party” means either EY or the Client.
- (j) “Personal Data” means Client Information relating to identified or identifiable natural persons or that is otherwise considered to be “personal data,” “personal information” or similar term under applicable data protection laws.
- (k) “Report(s)” means a Deliverable (or any portion of a Deliverable) issued on EY letterhead or under the EY brand or otherwise identifiable as being prepared by or in association with EY, any other EY Firm or EY Person.
- (l) Intentionally Omitted.
- (m) “Support Providers” means external service providers of EY and other EY Firms and their respective subcontractors.



(n) Intentionally Omitted.

### **Provision of the Services**

2. EY will provide the Services using reasonable skill and care in accordance with applicable professional standards.
3. EY may subcontract a portion of the Services to one or more EY Firms, as well as to other third parties, who may deal with the Client directly. EY will remain solely responsible to the Client for the performance of the Services. From time to time, non-CPA personnel may perform the Services.
4. EY will act as an independent contractor and not as the Client's employee, agent or partner. The Client will remain solely responsible for management decisions relating to the Services and for determining whether the Services are appropriate for its purposes. The Client shall assign qualified personnel to oversee the Services, as well as the use and implementation of the Services and Deliverables.
5. The Client agrees to promptly provide to EY (or cause others to so provide) Client Information, resources and assistance (including access to records, systems, premises and people) that EY requires to perform the Services.
6. The Client will ensure that the Client Information will be accurate and complete in all material respects. The provision of Client Information (including Personal Data), resources and assistance to EY will be in accordance with applicable law and will not infringe any copyright or other third-party rights.

### **Deliverables**

7. All Deliverables are intended for the Client's use in accordance with this Contract.
8. The Client may not rely on any draft Deliverable. EY shall not be required to update any final Deliverable as a result of circumstances of which EY becomes aware, or events occurring, after its delivery.
9. [Reserved]

### **Limitations**

10. As part of the parties' arrangements, the parties have mutually agreed the following limitations of liability (which also apply to others for whom Services are provided under this Contract):
  - a) Neither party will be responsible, in contract or tort, under statute or otherwise, for any amount with respect to loss of profit, data or goodwill, or any other consequential, incidental, indirect, punitive or special damages in connection with claims arising out of this Contract or otherwise relating to the Services, whether or not the likelihood of such loss or damage was contemplated.

- b) The Client (and any others for whom Services are provided) may not recover from EY, in contract or tort, under statute or otherwise, aggregate damages in excess of the fees actually paid for the Services that directly caused the loss under this Contract during the twelve (12) months preceding the date of the event giving rise to the loss. This cap is an aggregate cap across all claims under this Contract prior to such date.
  - c) The Client shall make any claim relating to the Services or otherwise under this Contract no later than one (1) year after the Client became aware (or ought reasonably to have become aware) of the facts giving rise to any alleged such claim and in any event, no later than two (2) years after the completion of the particular Services.
11. The limitations set out in Section 10 above will not apply to losses or damages caused by EY's fraud or willful misconduct or to the extent prohibited by applicable law or professional regulations.
12. The Client (and any others for whom Services are provided under this Contract) may not make a claim or bring proceedings relating to the Services or otherwise under this Contract against any other EY Firm or EY Person. The Client shall make any claim or bring proceedings only against EY.

#### **No Responsibility to Third Parties**

13. Unless specifically or otherwise agreed with the Client in writing, EY's responsibility for performance of the Services is to the Client and the Client alone. Should any Deliverable be disclosed, or otherwise made available, by or through the Client (or at the Client's request) to a third party (including but not limited to permitted disclosures to third parties as set forth in the Contract), the Client agrees to indemnify EY, as well as the other EY Firms and the EY Persons, against all claims by third parties, and resulting liabilities, losses, damages, costs and expenses (including reasonable external and internal legal costs) arising out of such disclosure.

#### **Intellectual Property Rights**

14. Each party retains its rights in its pre-existing intellectual property. Except as otherwise set out in this Contract, any intellectual property developed by EY, and any working papers compiled in connection with the Services (but not the Client Information contained in them), shall be the property of EY.
15. The Client's right to use Deliverables under this Contract arises following payment for the Services.

#### **Confidentiality, Data Protection & Security**

16. Except as otherwise permitted by this Contract, neither party may disclose to third parties any information provided by or on behalf of the other in connection with the Services (including, in the case of EY, Client Information). Either party may, however, disclose such information to the extent that it:
- (a) is or becomes public other than through a breach of this Contract;

- (b) is subsequently received by the recipient from a third party who, to the recipient's knowledge, owes no obligation of confidentiality to the disclosing party with respect to that information;
  - (c) was known to the recipient at the time of disclosure or is thereafter created independently;
  - (d) is disclosed as necessary to enforce the recipient's rights under this Contract; or
  - (e) must be disclosed under applicable law, legal process or professional regulations.
17. EY uses other EY Firms, EY Persons and Support Providers who may have access to Client Information in connection with delivery of Services as well as to provide Internal Support Services. EY shall be responsible for any use or disclosure of Client Information by other EY Firms, EY Persons or Support Providers to the same extent as if EY had engaged in the conduct itself.
18. The Client agrees that Client Information, including Personal Data, may be processed by EY, other EY Firms, EY Persons and their Support Providers in various jurisdictions in which they operate (EY office locations are listed at [www.ey.com](http://www.ey.com)). Client Information, including any Personal Data, will be processed in accordance with laws and professional regulations applicable to EY, and appropriate technical and organizational security measures designed to protect such information will be implemented. EY will also require any Support Provider that processes Personal Data on its behalf to provide at least the same level of protection for such Personal Data as is required by such legal and regulatory requirements. If Personal Data relating to a data subject in the UK, European Union or Switzerland (collectively, "European Personal Data") is required for EY to perform the Services, the parties agree to negotiate in good faith a data transfer addendum intended to validate the transfer of such European Personal Data by the Client to EY prior to such transfer. Transfer of Personal Data among members of the EY network is subject to the EY Binding Corporate Rules Program available at [www.ey.com/bcr](http://www.ey.com/bcr). Further information about EY's processing of Personal Data is available at [www.ey.com/privacy](http://www.ey.com/privacy).
19. To the extent permitted by applicable law, regulation or governmental directive, EY will notify the Client without undue delay in the event of loss, unauthorized disclosure or unauthorized or unlawful processing of Personal Data and provide the Client with relevant information about the nature and extent of the event.
20. In certain circumstances, individuals may have the right under applicable data protection law to access, correct, erase, port, restrict or object to the processing of their personal data. Such requests may be sent to [privacy.office@ey.com](mailto:privacy.office@ey.com). To the extent permitted by law, regulation or governmental directive, EY will notify the Client without undue delay upon receipt of any verifiable request from a data subject or supervisory authority relating to a Personal Data right. If EY is required to provide Personal Data in response to such verifiable request, or to a request from the Client, providing that data will be part of the Services and, to the extent permitted by applicable law, the Client will be responsible for EY's reasonable charges incurred in doing so.

21. As a professional services firm, EY is required to exercise its own judgment in determining the purposes and means of processing any Personal Data when providing the Services. Accordingly, unless otherwise specified in the Services Agreement, when processing Personal Data subject to the General Data Protection Regulation or other applicable data protection law (including, without limitation, state data protection (e.g., the California Consumer Privacy Act)), EY acts as an independent controller (or similar status that determines the purposes and means of processing), and not as a processor under the Client's control (or similar status acting on behalf of the Client) or as a joint controller with the Client. For Services where EY acts as a processor processing Personal Data on the Client's behalf, the parties will agree to appropriate data processing terms in the Services Agreement.
22. If the Client requires EY to access or use the Client or third-party systems or devices, to transmit, store and/or process Client confidential information, EY shall treat the Client confidential information consistent with the confidentiality obligations set forth in this Contract. The Client acknowledges and agrees that EY does not assume responsibility or liability of any kind for the confidentiality, practices, information security or data protection controls of such systems or devices, or for their performance or compliance with the Client requirements or applicable law.
23. EY may provide the Client access to use certain data, software, designs, utilities, tools, models, systems and other methodologies and know-how that EY owns or licenses for the purpose of the Client's receipt of the Services or as otherwise expressly agreed in writing by EY ("EY Tools"). The Client shall be responsible for compliance by all the Client personnel and third parties acting on the Client's behalf with the terms applicable to the use of such EY Tools. As between EY and the Client, EY (or another EY Firm) owns all right, title, interest, and all intellectual property rights in and to the EY Tools, including any enhancements, modifications, and derivative work thereof.

### **Compliance**

24. In connection with their respective rights and obligations under this Contract, EY and the Client each will comply with all laws, rules, and regulations of any jurisdiction applicable to it from time to time concerning or relating to: (i) bribery or corruption, including, without limitation, the U.S. Foreign Corrupt Practices Act ("FCPA"); (ii) anti-money laundering, including, without limitation the Bank Secrecy Act of 1970 and the USA PATRIOT Act of 2001, and (iii) economic or financial sanctions, export controls, trade embargoes or other similar prohibitions or restrictions on activity imposed by a government authority having jurisdiction over such party, including without limitation the U.S. Office of Foreign Assets Control ("OFAC") sanctions and the U.S. Export Administration Regulations ("EAR") (collectively, "Sanctions Laws"). The Client represents that it is not, nor is it 50% or more owned or otherwise controlled by a person or persons, subject to Trade Restrictions. The term "subject to Trade Restrictions," as applied to a person, means that such person falls into one or more of the following categories: (i) an individual located or ordinarily resident in, or an entity legally organized in a country listed on, any embargoed country list maintained by an applicable jurisdiction; (ii) an individual or entity listed on or covered by, or an entity 50% or more owned or otherwise controlled by a person or persons listed on or covered by, any sanctions asset blocking list, export denial list or other prohibited transactions list, directive, rule or regulation

maintained or issued by an applicable jurisdiction; or (iii) an individual or entity engaged in activities prohibited by the export controls or sanctions laws and regulations of an applicable jurisdiction. If the Client, or any agent, owner, investor, manager, partner, director, or officer of the Client or any beneficiary of the Services (including, without limitation, any affiliate of the Client), is or becomes subject to Trade Restrictions or if any of the Client's representations in this Section otherwise cease to be true at any time, then the Client shall notify EY immediately in writing. If the Client is an investment fund or fund manager, the Client represents that no limited partner or other partner, manager or investor within the fund is subject to Trade Restrictions (unless disclosed to EY in writing) and that the Services are not being used for the specific benefit of any party subject to Trade Restrictions. The Client further represents that the Client is not aware of any facts or circumstances that would cause EY, which is a U.S. person, to be in violation of any Sanctions Laws (including, without limitation, OFAC sanctions) in its performance of the Services. The Client shall not use the Services to circumvent, or facilitate any violation of, export controls or Sanctions Laws, or to facilitate any transaction with any person subject to Trade Restrictions. Notwithstanding anything to the contrary in this Contract, in the event that (1) any of the Client's representations in this Section cease to be true at any time for any reason (including, without limitation, any change in applicable law), (2) the Client otherwise breaches any of the provisions of this Section, or (3) EY determines any Services can no longer be performed as contemplated by this Contract due to the effects of Sanctions Laws or other applicable legal or regulatory restrictions on trade, then in each such case EY may immediately terminate this Contract, or any particular Services, in whole or in part. EY shall use commercially reasonable efforts to notify the Client of any Services that will no longer be provided as a result of any termination pursuant to this Section; provided that any failure to give any such notice shall not limit or otherwise affect the effectiveness of any such termination.

#### **Fees and Expenses Generally**

25. The Client shall pay EY's professional fees and specific expenses in connection with the Services as detailed in this Contract. The Client shall also reimburse EY for other reasonable expenses incurred in performing the Services. EY's fees are exclusive of taxes or similar charges, as well as customs, duties or tariffs imposed in respect of the Services, all of which the Client shall pay (other than taxes imposed on EY's income generally). Unless otherwise set forth in the Services Agreement, payment is due within forty-five(45) days following Client's receipt of each of EY's invoices.
26. EY may charge additional professional fees if events beyond its control (including the Client's acts or omissions) affect EY's ability to perform the Services as agreed in this Contract, or if the Client asks EY to perform additional tasks.
27. If EY is required by applicable law, legal process or government action to produce information or personnel as witnesses with respect to the Services or this Contract, the Client shall reimburse EY for any professional time and expenses (including reasonable external and internal legal costs) incurred to respond to the request, unless EY is a party to the proceeding or the subject of the investigation.

### **Force Majeure**

28. Neither party shall be liable for breach of this Contract (other than payment obligations) caused by circumstances beyond such party's reasonable control.

### **Term and Termination**

29. This Contract applies to all Services associated with this Contract whenever performed (including before the date of this Contract).
30. This Contract shall terminate on the completion of the Services associated with this Contract. Except as otherwise set forth in this Contract, either party may terminate this Contract, or any particular Services, upon thirty (30) days' prior written notice to the other. In addition, EY may terminate this Contract, or any particular Services, immediately upon written notice to the Client if EY reasonably determines that it can no longer provide the Services in accordance with applicable law or professional obligations.
31. The Client shall pay EY for all work-in-progress, Services already performed, and expenses incurred by EY up to and including the effective date of the termination or expiration of this Contract, as well as any applicable termination fees set forth in this Contract. Payment is due within forty-five (45) days following the date of the invoice for these amounts.
32. The term of this Contract will be as set forth in the Services Agreement (the "Term").
33. The provisions of this Contract, including Section 7 and 8 and otherwise with respect to Deliverables, that give either party rights or obligations beyond its termination shall continue indefinitely following the termination of this Contract.

### **Governing Law and Dispute Resolution**

34. This Contract, and any non-contractual matters or obligations arising out of this Contract or the Services, shall be governed by, and construed in accordance with, the laws of the state of New York applicable to agreements made, and fully to be performed, therein by residents thereof. Except for a claim seeking solely injunctive relief, any dispute relating to this Contract or the Services shall be resolved as set forth in **Appendix 1A**.

### **United States Specific Terms**

35. The U.S. Department of Labor (DOL) regulations, at 20 CFR § 655.734(a)(1)(ii)(A), require the posting of notice of a Labor Condition Application (LCA) in instances where individuals holding certain visas (e.g., H-1B) will be working onsite. Where applicable, EY and the Client will work together to develop an appropriate notice to enable compliance with this requirement.

### **Miscellaneous**

36. This Contract constitutes the entire agreement between the parties as to the Services and the other matters it covers, and supersedes all prior agreements, understandings and representations with respect thereto, including any previously agreed confidentiality agreements.
37. Each party may execute this Contract, as well as any modifications to this Contract, by electronic means, and each party may sign a different copy of the same document. Both parties must agree in writing to modify this Contract.
38. The Client agrees that EY and the other EY Firms may, subject to professional obligations, act for other clients, including the Client's competitors.
39. Neither party shall assign any of its rights or obligations under this Contract in whole or in part without the prior written consent of the other party; provided, however, that EY may assign or novate any of its rights and obligations under this Contract in whole or in part to (i) any other EY Firm and/or (ii) any entity resulting from, or established as part of, a restructuring, sale or transfer of an EY Firm, in whole or in part, provided further that any such assignment or novation does not materially affect continuity of the Services. EY shall provide the Client with notice of any such assignment or novation.
40. If any provision of this Contract (in whole or part) is held to be illegal, invalid or otherwise unenforceable, the other provisions shall remain in full force and effect.
41. The Client acknowledges that the U.S. Securities and Exchange Commission regulations indicate that, where auditor independence is required, certain confidentiality restrictions related to tax structure may render the auditor to be deemed to be non-independent or may require specific tax disclosures. Accordingly, if and only to the extent that U.S. Securities and Exchange Commission auditor independence regulations apply to the relationship between the Client or any of the Client's associated entities and any EY Firm, with respect to the tax treatment or tax structure of any transaction to which the Services relate, the Client represents, to the best of its knowledge, as of the date of this Contract, that neither the Client nor any Client Affiliate has agreed, either orally or in writing, with any other advisor to restrict the Client's ability to disclose to anyone such tax treatment or tax structure. The Client agrees that the impact of any such agreement is its responsibility.
42. The Client represents that Client Affiliates for whom Services are performed by EY in connection with this Contract shall be bound by the terms of this Contract.
43. Neither party may use or reference the other's name, logos or trademarks without its prior written consent, provided that EY may use the Client's name publicly to identify the Client as a client in connection with specific Services or otherwise.
44. The limitations in Sections 10 and 12 and the provisions of Sections 13, 18, 38 are intended to benefit the other EY Firms and all EY Persons, who shall be entitled to enforce them.

## APPENDIX 1A

### Dispute Resolution Procedures

#### Mediation

1. A party shall submit a dispute to mediation by written notice to the other party or parties. The mediator shall be selected by the parties. If the parties cannot agree on a mediator, the International Institute for Conflict Prevention and Resolution ("CPR") shall designate a mediator at the request of a party. Any mediator must be acceptable to all parties and must confirm in writing that he or she is not, and will not become during the term of the mediation, an employee, partner, executive officer, director, or beneficial owner with significant influence over any EY audit client or the parties to this Contract.
2. The mediator shall conduct the mediation as he/she determines, with the agreement of the parties. The parties shall discuss their differences in good faith and attempt, with the mediator's assistance, to reach an amicable resolution of the dispute. The mediation shall be treated as a settlement discussion and shall therefore be confidential. The mediator may not testify for either party in any later proceeding relating to the dispute. The mediation proceedings shall not be recorded or transcribed.
3. Each party shall bear its own costs in the mediation. The parties shall share equally the fees and expenses of the mediator.
4. If the parties have not resolved a dispute within 90 days after written notice beginning mediation (or a longer period, if the parties agree to extend the mediation), the mediation shall terminate and the dispute shall be settled by arbitration. In addition, if a party initiates litigation, arbitration, or other binding dispute resolution process without initiating mediation, or before the mediation process has terminated, an opposing party may deem the mediation requirement to have been waived and may proceed with arbitration.

#### Arbitration

5. The arbitration will be conducted in accordance with the procedures in this document and the CPR Rules for Non-Administered Arbitration ("Rules") as in effect on the date of the Agreement, or such other rules and procedures as the parties may agree. In the event of a conflict, the provisions of this document will control.
6. The arbitration will be conducted before a panel of three arbitrators, to be selected in accordance with the screened selection process provided in the Rules. Any issue concerning the extent to which any dispute is subject to arbitration, or concerning the applicability, interpretation, or enforceability of any of these procedures, shall be governed by the Federal Arbitration Act and resolved by the arbitrators. No potential arbitrator may be appointed unless he or she has agreed in writing to these procedures



and has confirmed in writing that he or she is not, and will not become during the term of the arbitration, an employee, partner, executive officer, director, or beneficial owner with significance influence over any EY audit client or the parties to this Contract.

7. The arbitration panel shall have no power to award non-monetary or equitable relief of any sort or to make an award or impose a remedy that (i) is inconsistent with the agreement to which these procedures are attached or any other agreement relevant to the dispute, or (ii) could not be made or imposed by a court deciding the matter in the same jurisdiction. In deciding the dispute, the arbitration panel shall apply the limitations period that would be applied by a court deciding the matter in the same jurisdiction, and shall have no power to decide the dispute in any manner not consistent with such limitations period.
8. Discovery shall be permitted in connection with the arbitration only to the extent, if any, expressly authorized by the arbitration panel upon a showing of substantial need by the party seeking discovery.
9. All aspects of the arbitration shall be treated as confidential. The parties and the arbitration panel may disclose the existence, content or results of the arbitration only in accordance with the Rules or applicable professional standards. Before making any such disclosure, a party shall give written notice to all other parties and shall afford them a reasonable opportunity to protect their interests, except to the extent such disclosure is necessary to comply with applicable law, regulatory requirements or professional standards.
10. The result of the arbitration shall be binding on the parties, and judgment on the arbitration award may be entered in any court having jurisdiction.