Code of Practice on Disinformation – January 2023 Baseline Report of Adobe for the period [16 Dec 2022 – 16 January 2023]

Table of Content

II. Scrutiny of Ad Placements	1
Commitment 1	1
Commitment 2	4
Commitment 3	5
III. Political Advertising	Error! Bookmark not defined.
Commitment 4	Error! Bookmark not defined.
Commitment 5	Error! Bookmark not defined.
Commitment 6	Error! Bookmark not defined.
Commitment 7	Error! Bookmark not defined.
Commitment 8	Error! Bookmark not defined.
Commitment 9	Error! Bookmark not defined.
Commitment 10	Error! Bookmark not defined.
Commitment 11	Error! Bookmark not defined.
Commitment 12	Error! Bookmark not defined.
Commitment 13	Error! Bookmark not defined.
IV. Integrity of Services	Error! Bookmark not defined.
Commitment 14	Error! Bookmark not defined.
Commitment 15	Error! Bookmark not defined.
Commitment 16	Error! Bookmark not defined.
V. Empowering Users	Error! Bookmark not defined.
Commitment 17	Error! Bookmark not defined.
Commitment 18	Error! Bookmark not defined.
Commitment 19	Error! Bookmark not defined.
Commitment 20	6
Commitment 21	Error! Bookmark not defined.
Commitment 22	Error! Bookmark not defined.
Commitment 23	Error! Bookmark not defined.
Commitment 24	Error! Bookmark not defined.
Commitment 25	Error! Bookmark not defined.
VI. Empowering the research community	Error! Bookmark not defined.
Commitment 26	Error! Bookmark not defined.
Commitment 27	Error! Bookmark not defined.
Commitment 28	Error! Bookmark not defined.
Commitment 29	Error! Bookmark not defined.

VII. Empowering the fact-checking community	Error! Bookmark not defined.
Commitment 30	Error! Bookmark not defined.
Commitment 31	Error! Bookmark not defined.
Commitment 32	Error! Bookmark not defined.
Commitment 33	Error! Bookmark not defined.
VIII. Transparency Centre	9
Commitment 34	9
Commitment 35	9
Commitment 36	9
IX. Permanent Task-Force	10
Commitment 37	10
X. Monitoring of Code	11
Commitment 38	11
Commitment 39	11
Commitment 40	11
Commitment 41	Error! Bookmark not defined.
Commitment 42	Error! Bookmark not defined.
Commitment 43	Error! Bookmark not defined.
Commitment 44	Error! Bookmark not defined.

Executive summary

Adobe has been a proud Signatory of the EU Code of Practice on Disinformation since June 2022 and we support the intention and ambition of this Code.

Adobe is a global leader in digital marketing and digital media solutions. Since the company's foundation in December 1982, we have pushed the boundaries of creativity with products and services that allow our customers to create, deploy, and enhance digital content. Our purpose is to serve the creator and respect the consumer, and our heritage is built on providing trustworthy and innovative solutions to our customers.

With the increasing volume and velocity of digital content creation, including synthetic media, it is critical to ensure transparency, understanding, and trust in what we are consuming online while empowering consumers. Adobe feels a responsibility to support the creative community, and society at large, and is committed to finding solutions that address the issues of manipulated media and tackle disinformation.

As such, content provenance is a major focus for Adobe and the work we lead on the Content Authenticity Initiative (CAI). We are focused on cross-industry participation, with an open, extensible approach for providing media transparency to allow for better evaluation of content.

The CAI advocates for a set of open standards that can be used to create and reveal provenance for images, documents, time-based media (video, audio) and streaming content. Provenance, sometimes referred to as attribution, empowers content creators, editors, and publishers, regardless of their geographic location or degree of access to technology, to voluntarily disclose information about who created or changed an asset, what was changed and how it was changed.

In February 2021, Adobe, Arm, BBC, Intel, Microsoft, and Truepic launched a formal coalition for standards development: The Coalition for Content Provenance and Authenticity (C2PA). The C2PA is a mutually governed consortium created to accelerate the pursuit of pragmatic, adoptable standards for digital provenance, serving creators, editors, publishers, media platforms, and consumers.

In January 2022, the C2PA publicly released the open technical specification for digital provenance, which provides platforms with a blueprint to define what information is associated with each type of asset (e.g., images, videos, audio, or documents), how that information is presented and stored, and how evidence of tampering can be identified.

This work will continue to evolve and address the latest trends and landscape needs. We see Adobe's work on content provenance being particularly relevant to the EU Code of Practice on Disinformation and are grateful that Commitments relating to provenance and the C2PA open standard have been adopted as commitments in the Code in the Empowering Users chapter. We encourage all relevant Signatories to sign up to these commitments and join this cross-industry effort to tackle disinformation through the use of technology.

Guidelines for filling out the report

Baseline reports are detailing how Signatories have implemented their Commitments under the Code and provide the Qualitative Reporting Elements (QREs) and Service Level Indicators (SLIs), as they stand one month after the implementation. The baseline report should also include a comparison between the measures in place under the previous Code to the measures taken to implement the new Code. The measures taken to implement the new Code should be outlined per commitment in the dedicated field of the reporting template.

Reporting period

The reporting period to be covered in the baseline reports is from 16 December 2022 to 16 January 2023 for all Signatories. (The implementation period of the Code from 16 June 2022 to 16 December 2022 is followed by a one-month reporting period from 16 December 2022 to 16 January 2023.) Signatories shall submit baseline reports outlining policy updates and actions taken to implement the Code during the implementation period. Data, e.g. on the number of actions taken under a specific policy, should be reported on from the end of the implementation period (16 December 2022) until the cut-off date of 16 January 2023. In case specific data is not available for the first reporting period (from 16 December 2022 to 16 January 2023), please provide the monthly average based on the previous quarter, clearly outlining the methodology used in the relevant field. The submission date for baseline reports is January 31, 2023.

Adjusting the reporting template

Non-VLOPs can adapt the template to specific commitments and measures they subscribed to. This may include adapted wording for commitments, measures, QREs and SLIs. Non-VLOPs signatories will report only on commitments and measures they subscribed to and provide Member State-level data only if feasible.

Reporting per Service

When filling in a report for several services, use colour codes to clearly distinguish between services. At the beginning of the report, clarify what colour is used for which service.

Reporting in text form

Reporting in the form of written text is required for several parts of the report. Most of them are accompanied by a target character limit. Please stick to the target character limit as much as possible. We encourage you to use bullet points and short sentences. Links should only be used to provide examples or to illustrate the point. They should not be used to replace explanations or to provide data in the forms. All relevant explanations and data must be included in the table directly, in written form.

Reporting SLIs and data

Reporting on Service Level Indicators requires quantitative information to be reported in the reporting template. We ask you to report data in the format provided by the reporting template, not on external links.

Reporting on TTPs

If subscribed to Commitment 14, Integrity of Services, we ask you to report on each identified TTP individually. The number of identified TTPs may vary per service. Where more than one TTP are reported under the same action, clarify the reasoning in the methodology. Where input is not provided, keep the placeholder for the relevant TTP and explain reasons and planned remedial action. Additionally, as with all other SLIs, data can be provided per Member State for each individual TTP.

Missing Data

In case that at the time of reporting there is no data available yet, the data is insufficient or the methodology is lacking, please outline in the dedicated field (i.e. in the field about further implementation measures planned) how this will be addressed over the upcoming six months, being as specific as possible. Please also indicate inconsistencies or gaps regarding methodology in the field dedicated to methodology.

Attachments

We ask you not to enclose any additional attachments to the harmonised reporting template.

Uploading data to the Transparency Centre

After the submission of the baseline reports and the launch of the Transparency Centre website, all data from the reporting template must be uploaded to the Transparency Centre within maximum 7 days, allowing easy data access and filtering. It is the responsibility of the Signatories to ensure that the uploading takes place and is executed on time. Signatories are also responsible to ensure that the Transparency Centre is operational and functional by the time of the reports' submission, that the data from the reports are uploaded and made accessible in the Transparency Centre within the above deadline, and that users are able to read, search, filer and download data as needed in a user-friendly way and format.

II. Scrutiny of Ad Placements Commitment 1 Relevant signatories participating in ad placements commit to defund the dissemination of disinformation, and improve the policies and systems which determine the eligibility of content to be monetised, the controls for monetisation and ad placement, and the data to report on the accuracy and effectiveness of controls and services around ad placements. [change wording if adapted] [insert wording if adapted] Measure 1.1 **QRE 1.1.1** [insert Adobe Advertising Clouds' Ads Requirements Policy outlines the requirement for ads to not be "False or misleading ads", accounting for wording if adapted] both misinformation and disinformation. In Summer, 2020, Adobe halted working with political advertisers. Actions taken are the following. (1) A Framework for tracking reported incidents has been built. (2) Past examples of reported incidents of Mis/Disinformation have been added to a master tracker. (3) The process by which incidents are reported, steps taken to block them, are outlined in an internal Wiki. (4) Incidents found during the first period of submission have been added to the tracker. (5) Adobe Advertising Cloud has reached out to existing partners for consult on available services with relevant solutions to combatting dis/misinformation. No new services have been on-boarded. Link to ads requirements policy: https://experienceleague.adobe.com/docs/advertising-cloud/policies/ad-requirements-policy.html?lang=en Methodology of data measurement [suggested character limit: 500 characters] Type of Action 3 [linked to the 8 Domains from GDI's "Ad-Funded Type of Action 2 [linked to the policy Type of Action 4 [linked to the SLI 1.1.1 mentioned in ORE1 policy mentioned in QRE] policy mentioned in QRE] Disinformation: Misogyny" have **Numbers by** been added to Adobe's platform actions enforcing blocklist. This block list affects all policies above (specify if at page transparent open market and/or domain advertising. level) [change wording if adapted] Level domain Page/Domain Page/Domain Page/Domain Data redstate.com washingtonexaminer.com thefederalist.com

theepochtimes.com

	pjmedia.com		
	newsbusters.org		
	m.washingtonexaminer.com		
Member States	Not available		
[example, insert only			
if feasible]			
Austria			
Belgium			
Bulgaria			
Croatia			
Cyprus			
Czech Republic			
Denmark			
Estonia			
Finland			
France			
Germany			
Greece			
Hungary			
Ireland			
Italy			
Latvia			
Lithuania			
Luxembourg			
Malta			
Netherlands			
Poland			
Portugal			
Romania			
Slovakia			
Slovenia			
Spain			
Sweden			
Iceland			
Liechtenstein			
Norway			

Total EU			1	
Total EEA				
1.1.1). It is based on	-	ries (query/bid¹ or impressior		onetise disinformation sources (under SLI onversion factor provided by a third party
SLI 1.1.2 - Preventing the flow of legitimate advertising investment to sites		is done by pulling historical in	characters] npression delivery on sites, apps, or tion to determine final value in Eur	
or content that are designated as disinformation [change wording if adapted]	Euro value of ads demonetised Please see above.			
Data				
Measure 1.2	[insert wording if adapted]			
QRE 1.2.1 [insert wording if adapted]	Adobe Ad Cloud does not work w	ith political advertisers.		
SLI 1.2.1 [change	Methodology of data measurement [suggested character limit: 500 characters]			
wording if adapted]	No policies have been updated, added, or removed.	Nr of update to policies	Nr of accounts barred	Nr of domains barred
Data				
Measure 1.3	[insert wording if adapted]			
QRE 1.3.1 [insert wording if adapted]	Advertisers are provided Advertisers are automativiolate policies or are deadvertiser has manually of	reporting on standard deliver cally opted into Adobe Ad Clo termined to be inappropriate to opted out or (2) the advertiser	uds "Global Blocklist" which includ or advertising. This prevents ad del	very, at a site domain and app level. es reviewed sites and apps determined to livery on those properties (1) unless the osed to or not transparent with these

¹ Request placed between a seller and buyer of advertising that can detail amongst other things website, specific content, targeting data inclusive of audience or content.

² Comprehensive calculation of the number of people who have been reached by a piece of media content by passive exposure (viewing a piece of content) or active engagement (visiting a destination).

Measure 1.6	[insert wording if adapted]
QRE 1.6.1 [insert	Adobe Ad Cloud offers several 3 rd Party brand-safety targeting services that can be applied to campaign placements through our partners,
wording if adapted]	with a fee. Pre-bid services halt impression delivery at the app, site or page level. These services are optional.

		II. Scrutiny of Ad Placem	ents	
		Commitment 2		
Relevant Signatories p	. 2	•	ertising systems to disseminate D	Disinformation in the form of
		ising messages. [change wordin	g if adapted]	
Measure 2.1	[insert wording if adapted]			
QRE 2.1.1 [insert wording if	Adobe Advertising Clouds adve	tising policy clearly states that Fa	alse or Misleading ads are prohibi	ted. Additionally Political ads are
adapted]	prohibited.			
			licies/ad-requirements-policy.htm	•
	If an ad is found or reported to be in violation of the Ads Requirements Policy, the ad placement is paused, the Advertiser is notified to			
		s Ads Requirements Policy. If three	separate event violations are found	from the same advertiser, they will
	be removed from the platform.	I =	T- 64 11 0 511 1 1 1 1	
SLI 2.1.1 – Numbers by	Between October 1, 2022 and	Type of Action 2 [linked to the	Type of Action 3 [linked to the	Type of Action 4 [linked to the
actions enforcing policies	December 24, 2023, no advertisers have been found to	policy mentioned in QRE]	policy mentioned in QRE]	policy mentioned in QRE]
above [change wording if	violate Adobe Advertising			
adapted]	Cloud's advertising policy. We			
	do not currently have data			
	available for December 16,			
	2022 to January 16 2023.			
Data				
Measure 2.2	[insert wording if adapted]			
QRE 2.2.1 [insert wording if	Adobe Advertising Cloud is assessing services available from current and new partners for disinformation or misinformation. This			
adapted]	includes block lists, measurement or reporting, and pre-bid services.			
Measure 2.3	[insert wording if adapted]			
Measure 2.4	[insert wording if adapted]	[insert wording if adapted]		
QRE 2.4.1 [insert wording if			licy, they are notified via email. T	
adapted]	in violation, the policy it violates, and a link to Adobe's Ads Requirements Policy. They are also notified that three violations may			
adapted	result in removal from the platfo	orm.		

Advertisers can appeal this process and be subject to a 90 day grace period to be reviewed if any additional violations are levied against them. The strikes may be removed after these conditions are met.

II. Scrutiny of Ad Placements

Commitment 3

Relevant Signatories involved in buying, selling and placing digital advertising commit to exchange best practices and strengthen cooperation with relevant players, expanding to organisations active in the online monetisation value chain, such as online e-payment services, e-commerce platforms and relevant crowd-funding/donation systems, with the aim to increase the effectiveness of scrutiny of ad placements on their own services. [change wording if adapted]

Measure 3.1	[insert wording if adapted]
QRE 3.1.1 [insert wording if adapted]	Adobe Advertising Cloud has partnerships with various 3rd party brand safety solution providers to offer targeting and reporting. Some have available targeting related to disinformation and misinformation. Adobe Advertising Cloud cooperates with supply partnerships to block any apps, sites, or sellers that are found to have disinformation and misinformation. Adobe Ad Cloud also reviews publicly available reports through reputable journals or news articles establishing specific acts of disinformation or misinformation.
Measure 3.2	[insert wording if adapted]
QRE 3.2.1 [insert wording if adapted]	We have reached out to a third party provider offering misinformation and disinformation review of third party sites and apps. This provider could provide lists that we may add to Adobe's Global Blocklist.
Measure 3.3	[insert wording if adapted]
QRE 3.3.1 [insert wording if adapted]	Adobe Advertising Cloud has integrated at least 8 domains found on publicly available reports from the potential partner referred to in QRE 3.2.1 to begin to demonetize distributors of dis/misinformation.

V. Empowering Users

Commitment 20

Relevant Signatories commit to empower users with tools to assess the provenance and edit history or authenticity or accuracy of digital content. [change wording if adapted]

Measure 20.1

QRE 20.1.1 [insert wording if adapted]

Open-source tools released:

In June 2022, Adobe released a suite of <u>open-source developer tools</u> based on the Coalition for Content Provenance and Authenticity (C2PA) specification, enabling more developers to integrate content provenance across web, desktop, and mobile projects — for free. This is helping to get provenance tools into the hands of millions of creators and developers to create a safer, more transparent digital ecosystem, while providing users with information to be better informed about the content they see online.

Adobe's Content Credentials team supports three options for open-source tools to implement C2PA standards beyond just Adobe apps. These tools include options from lightweight JavaScript to read Content Credentials on your site or app to completely customisable tools with the full SDK. From our original release of the open-source tools earlier this year, the tools now have both updated documentation and quicker file processing time to improve the developer experience. Support for selected video and audio formats, and mobile development, as we continue to explore how we can expand content provenance to new mediums.

Provenance tool available in Photoshop:

Adobe has used the C2PA technical standards published in early 2022 and launched a provenance feature in its flagship creative media tool, Photoshop, called Content Credentials, in private beta in 2021. In October 2022 we announced further improvements and is now available, for free, to millions of Photoshop subscribers (individual and enterprise) globally as an opt-in feature. When enabled, the feature captures edits and identity information from a working image. A user can then attach this information to the image when exporting it. This secure metadata provides new transparency options for creative professionals, and photojournalists, while also reinforcing trust in digital content for the people viewing it. For more information available here.

Also in October 2022, we announced the new Content Credentials cloud, where users can publish their Content Credentials (provenance and edit history) which enables search and recovery so that audiences can see the original Content Credentials, even if they have been maliciously or accidentally stripped off. Exporting to Content Credentials cloud allows the provenance of any creator's work to be permanently available for cases where metadata is removed or damaged, strengthening creator attribution.

Additionally, <u>Adobe Stock</u>, which supplies hundreds of thousands of assets to customers daily, has adopted Content Credentials to provide provenance data for all image assets, and <u>Behance</u>, Adobe's community platform for creators displays Content Credentials so that viewers of Behance content can understand its origins and context.

We are working hard in 2023 to raise more awareness of this opt-in feature and explain its important role in helping users check the authenticity of digital content. We also have a roadmap to integrate Content Credentials in other Adobe products in 2023, including Imaging, video, and 3D offerings.

Provenance for audiences everywhere:

The Adobe team has also developed <u>Verify</u>, a website where consumers can see important provenance information about a piece of digital content. When false narratives or misleading information go viral, we often "Google" to compare coverage and cross-check available information. This common behaviour and digital provenance history drive Verify, where anyone can upload an image to trace the history and edits made to a piece of digital content. In October 2022, we updated the website to support the search and recovery of provenance and attribution history from Content Credentials cloud. This allows for the ground-breaking ability to ensure Content Credentials are permanently associated with your content, no matter where it travels.

Supporting implementation in cameras:

Throughout 2022, Adobe partnered with two industry-leading camera manufacturers, Leica and Nikon, to integrate provenance technology into their camera hardware, using both the C2PA standard, and our open-source developer tools. These devices were exhibited in October 2022 at the Adobe MAX conference.

This partnership implements provenance technology into two cameras: Leica's iconic M11 Rangefinder and Nikon's industry-leading mirrorless camera, the Nikon Z9, enabling their global customer base to attach provenance to their images at the point of capture, creating a chain of authenticity from camera to cloud. Further information on this exciting partnership is available in our <u>press release</u> and <u>blog</u>.

	This milestone will allow photographers and creators alike to increase trust in their digital work by securely attaching valuable provenance information at the point of capture, including when, where and how each image was created. These details establish an image's attribution and trustworthiness from the start, which helps protect against the spread of misinformation by empowering consumers to identify the origins and edit history throughout the digital content lifecycle. We are excited and proud of this partnership as it shows this open standard technology can be implemented in both software and hardware. It was also relatively straightforward to do with low resource and time needed which is encouraging for the goal of ubiquitous adoption across the eco-system, including relevant signatories of the Code.
Measure 20.2	
QRE 20.2.1 [insert wording if adapted]	Outline relevant actions [suggested character limit: 2000 characters]
	Adobe founded the <u>Content Authenticity Initiative</u> (CAI) in late 2019. The CAI is an Adobe-led initiative with more than 900 partners working to increase trust online through provenance, which are the facts about the origins of a piece of digital content. We welcomed many new CAI members this year—leading publishers and visual content providers including the Associated Press, Agencia EFE, El Tiempo, EPA Images, Reuters and the Wall Street Journal to name a few. Internally, at Adobe we have a team of full time employees dedicated to working on CAI. This includes engineers helping to develop and maintain our open-source tooling for the community, user-experience designers, and a team dedicated to recruiting partners, supporting adoption and growing the community globally.
	In addition, Adobe is an active member of the independent standards organisation, the <u>Coalition of Content Provenance and Authenticity</u> , and sits on the Steering Committee which meets weekly, Chairs and the Technical Working Group and has representatives on the Threats and Harms Task Force and support from Adobe employees from our Communications and Policy team for C2PA external engagement. We are committed to working with other C2PA members such as Microsoft, BBC, ARM, Intel and Sony to ensure open technical standards for provenance are maintained to the highest standards and used to develop and implement content provenance across the eco-system which is interoperable and ultimately adopted by international standards organisations as the gold standard for this technology to tackle disinformation by empowering users with provenance tools.

VIII. Transparency Centre

Commitment 34

To ensure transparency and accountability around the implementation of this Code, Relevant Signatories commit to set up and maintain a publicly available common Transparency Centre website. [change wording if adapted]

Measure 34.1	[insert wording if adapted]
Measure 34.2	[insert wording if adapted]
Measure 34.3	[insert wording if adapted]
Measure 34.4	[insert wording if adapted]
Measure 34.5	[insert wording if adapted]

VIII. Transparency Centre

Commitment 35

Signatories commit to ensure that the Transparency Centre contains all the relevant information related to the implementation of the Code's Commitments and Measures and that this information is presented in an easy-to-understand manner, per service, and is easily searchable. [change wording if adapted]

Measure 35.1	[insert wording if adapted]
Measure 35.3	[insert wording if adapted]
Measure 35.5	[insert wording if adapted]
Measure 35.6	[insert wording if adapted]

VIII. Transparency Centre

Commitment 36

Signatories commit to updating the relevant information contained in the Transparency Centre in a timely and complete manner. [change wording if adapted]

Measure 36.1	[insert wording if adapted]
Measure 36.2	[insert wording if adapted]

IX. Permanent Task-Force

Commitment 37

Signatories commit to participate in the permanent Task-force. The Task-force includes the Signatories of the Code and representatives from EDMO and ERGA. It is chaired by the European Commission, and includes representatives of the European External Action Service (EEAS). The Task-force can also invite relevant experts as observers to support its work. Decisions of the Task-force are made by consensus. [change wording if adapted]

Measure 37.1	[insert wording if adapted]
Measure 37.2	[insert wording if adapted]
Measure 37.3	[insert wording if adapted]
Measure 37.4	[insert wording if adapted]
Measure 37.5	[insert wording if adapted]
Measure 37.6	[insert wording if adapted]
QRE 37.6.1 [insert wording if adapted]	Outline relevant actions [suggested character limit: 2000 characters] Adobe has participated in two of the four Taskforce Plenary meetings in Brussels and has attended the Monitoring and Reporting Taskforce meetings on an ad-hoc basis. In addition, Adobe has liaised with IAB who has been representing its members in the Ad Placements Taskforce.

X. Monitoring of Code

Commitment 38

The Signatories commit to dedicate adequate financial and human resources and put in place appropriate internal processes to ensure the implementation of their commitments under the Code. [change wording if adapted]

Measure 38.1	[insert wording if adapted]
QRE 38.1.1 [insert wording if adapted]	Adobe has created an EU Code of Practice Tiger Team, which is an internal, cross-functional team that
	meets regularly to discuss the implementation of the Code commitments and our reporting
	requirements. This work is then overseen by our General Counsel.

X. Monitoring of Code

Commitment 39

Signatories commit to provide to the European Commission, within 1 month after the end of the implementation period (6 months after this Code's signature) the baseline reports as set out in the Preamble. [change wording if adapted]

X. Monitoring of Code

Commitment 40

Signatories commit to provide regular reporting on Service Level Indicators (SLIs) and Qualitative Reporting Elements (QREs). The reports and data provided should allow for a thorough assessment of the extent of the implementation of the Code's Commitments and Measures by each Signatory, service and at Member State level. [change wording if adapted]

Measure 40.2	[insert wording if adapted]
Measure 40.3	[insert wording if adapted]
Measure 40.4	[insert wording if adapted]
Measure 40.5	[insert wording if adapted]
Measure 40.6	[insert wording if adapted]