Code of Practice on Disinformation – Report of Adobe for the period 1 January 2023 – 31 December 2023

Table of Content

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 experiences. 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 and communities. Adobe has a long history of pioneering innovation: when Adobe thinks about AI, we balance innovation with responsible innovation.

We are witnessing extraordinary challenges to trust in digital content. As social platforms amplify the reach and influence of certain content, mis-attributed and mis-contextualized content spreads quickly. Whether inadvertent misinformation or deliberate deception, inauthentic content is on the rise.

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

Content provenance and media literacy are a major focus for Adobe and the work of the Content Authenticity Initiative (CAI), which Adobe co-founded in 2019. We are focused on cross-industry participation, with an open, extensible approach for providing transparency for digital content (i.e. images, audio, video, documents, and generative AI) to allow for better evaluation of that content. The Content Authenticity Initiative (CAI) now has close to 2,500 members working to increase trust in digital content through provenance tools, which are the facts about the origins of a piece of digital content.

The CAI works in tandem with the Coalition for Content Provenance and Authenticity (C2PA), an open technical standards organization also co-founded by Adobe in 2021, to implement our solution to combating misinformation online – called Content Credentials. Content Credentials are essentially a "nutrition label" for digital content – showing when a piece of content is created and modified, including whether AI is used. Content Credentials are a combination of cryptographic metadata and watermarking, designed to remain securely attached and to travel with the digital content wherever it goes. They include important information which may include the creator's name, the date an image was created, what tools were used to create an image and any edits that were made along the way. This empowers users to create a digital chain of trust and authenticity. The CAI developed free, open-source tools based on the C2PA standard for anyone to implement Content Credentials into their own products, services, or platforms.

In the first months of 2024, several major developments concerning the C2PA took place, with Google joining the C2PA steering committee, OpenAI announcing the support of the C2PA standard and Content Credentials for images generated by DALL·E 3 and Meta announcing its plan to build on the C2PA's industry standard solution for adding provenance to content.

The Adobe-led CAI has also invested in creating and promoting media literacy curricula to educate the public about the dangers of deepfakes, the need for scepticism, and tools available today to help them understand what is true. In partnership with the Adobe Education team, the CAI updated their media literacy curriculum in February 2024 to include Generative AI curricular materials.

This open standard is more important than ever as powerful technology like Generative AI makes it easier to create, scale, and alter digital content and our work will continue to evolve and address the

latest trends and landscape needs. We see Adobe's focus on supporting and promoting wide adoption of content provenance tools as 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 technology.

Guidelines for filling out the report

Reports are detailing how signatories have implemented their Commitments under the Code and 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.

Reporting period

The reporting period to be covered in the reports is 12 months for signatories who are not offering very large online platform services. Signatories shall submit reports outlining policy updates and actions taken to implement the Commitments and Measures they signed up to under the Code. All data and policy updates should be reported for 12 months period from the submission of last reports.

Adjusting the reporting template

Signatories who are not offering very large online platform services can adapt the template to specific commitments and measures they subscribed to. This may include adapted wording for commitments, measures, QREs and SLIs. Relevant 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. When providing information to the QRE, please make sure that your answer covers all the elements of the associated commitment and measure. 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 report directly, in written form.

Reporting SLIs and data

Reporting on SLIs requires quantitative information to be reported on in this harmonised reporting template.

- Where relevant and feasible, SLIs should be reported on per Member State.
- If no data is available on Member State level, SLIs might, instead, be exceptionally reported on per language. (NB that signatories agreed to revisit this issue after the first reporting, to ensure harmonised and meaningful reporting.)
- Please report data in the format provided by the harmonised reporting template, not through external links. Please use the Member State/language template provided in the harmonised reporting template. Where the table asks for "Other relevant metrics", please name the metric that you would like to report on in addition to the ones already provided. You may include more than the number of additional fields provided where necessary; in that case, please adjust the table as needed.
- Please contextualize all data as much as possible, i.e. include baseline quantitative information that will help contextualize the SLIs (e.g. number of pieces of content labelled out of what volume of content).

- If there are no relevant metrics to report on, please leave the respective columns blank.

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.

Signatories are encouraged to provide insights about the data/numbers they provide by inserting possible explanations in the boxes of the template "*Methodology of data measurement & insights on data provided*". This should aim to explain the why of what is being reported, for instance - *Are there trends or curiosities that could require or use contextual explanation? What may be driving the change or the difference in the number?* Please also indicate inconsistencies or gaps regarding methodology in the dedicated box.

Attachments

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

Crisis and elections reporting template

Relevant signatories are asked to provide proportionate and appropriate information and data during a period of crisis and during an election. Reporting is a part of a special chapter at the end of the harmonised reporting template and should follow the guidelines:

- The reporting of signatories' actions should be as specific to the particular crisis or election reported on as possible. To this extent, the rows on "Specific Action[s]" should be filled in with actions that are either put in place specifically for a particular event (for example a media literacy campaign on disinformation related to the Ukraine war, an information panel for the European elections), or to explain in more detail how an action that forms part of the service's general approach to implementing the Code is implemented in the specific context of the crisis or election reported on (for example, what types of narratives in a particular election/crisis would fall into scope of a particular policy of the service, what forms of advertising are ineligible).
- Signatories who are not offering very large online platform services and who follow the invitation to report on their specific actions for a particular election or crisis may adapt the reporting template as follows:
    - They may remove the "Policies and Terms and Conditions" section of the template, or use it to report on any important changes in their internal rules applicable to a particular election or crisis (for example, a change in editorial guidelines for fact-checkers specific to the particular election or crisis)
    - They may remove any Chapter Section of the Reporting Template (Scrutiny of Ads Placement, Political Advertising, Integrity of Services etc.) that is not relevant to their activities

- The harmonised reporting template should be filled in by adding additional rows for each item reported on. This means that rather than combined/bulk reporting such as "Depending on severity of violation, we demote or remove content based on policies X, Y, Z", there should be individual rows stating for example "Under Policy X, content is demoted or removed based on severity", "Under Policy Y, content […]" etc.
- The rows should be colour-coded to indicate which service is being reported on, using the same colour code as for the overall harmonised reporting template.

Reporting should be brief and to the point, with a suggested character limit entry of 2000 characters.

Uploading data to the Transparency Centre

The reports should be submitted to the Commission in the form of the pdf via e-mail to the address CNECT COP TASK FORCE CNECT-COP-TASK-FORCE@ec.europa.eu within the agreed deadline. Signatories will upload all data from the harmonised reporting template to the Transparency Centre, allowing easy data access and filtering within the agreed deadline. 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]				
Measure 1.1	[insert wording if adapted]			
QRE 1.1.1 [insert wording if adapted]	**Adobe Advertising Clouds' Ads Requirements Policy outlines the requirement for ads to not be "False or misleading ads", accounting for both misinformation and disinformation. In Summer, 2020, Adobe halted working with political advertisers.** **Actions taken are the following:** **(1) Research was done to locate sites that spread Misinformation and Disinformation by referencing 3rd party reports from Global Disinformation Index, CheckMyAds and MediaBiasFactCheck.** **(2) Flagged Sites were reviewed and verified through manual checks of 3rd party verification services such as Global Disinformation Index and MediaBiasFactCheck.** **(3) Domains where Misinformation or Disinformation was confirmed were added to platforms Global Blocklist.** **(4) Historical impression reports are pulled to assess the impression delivery on the domains** **(5) Incidents found during the second period of submission have been added to the tracker.** **(6) Adobe Advertising Cloud has reached out to existing partners for consultation 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			
SLI 1.1.1 – Numbers by actions enforcing policies above (specify if at page and/or domain level) [change wording if adapted]	Methodology of data measurement [suggested character limit: 500 characters]			
	7 Domains have been added to Adobe's platform blocklist. This block list affects all transparent open market advertising.	Type of Action 2 [linked to the policy mentioned in QRE]	Type of Action 3 [linked to the policy mentioned in QRE]	Type of Action 4 [linked to the policy mentioned in QRE]
Level	Domain	Page/Domain	Page/Domain	Page/Domain
Data				

Member States [example, insert only if feasible]	Not available			
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				
Total EEA				

This additional Service Level Indicator provides an estimated financial value of the actions taken by Signatories to demonetise disinformation sources (under SLI 1.1.1). It is based on media metrics available to Signatories (query/bid[1] or impression[2]) and applying an agreed-upon conversion factor provided by a third party designated by the Task-force of the Code (Ebiquity plc.).	
SLI 1.1.2 - Preventing the flow of legitimate advertising investment to sites or content that are designated as disinformation [change wording if adapted]	**Methodology of data conversion is done by pulling historical impression delivery on sites, apps, or ads verified as having dis/misinformation and using Ebiquity's conversion rate calculation to determine final value in Euros.**
	See response above
Data	
Measure 1.2	[insert wording if adapted]
QRE 1.2.1 [insert wording if adapted]	**Adobe Ad Cloud does not work with political advertisers. Adobe Ad Cloud is a member of the IAB Tech Lab, Network Advertising Initiative (NAI), Digital Advertising Alliance (DAA), European Interactive Digital Advertising Alliance (EDAA), and Trustworthy and Accountability Group (TAG).**
SLI 1.2.1 [change wording if adapted]	Methodology of data measurement [suggested character limit: 500 characters]

[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).

	No policies have been updated, added, or removed.	Nr of update to policies **None at this time.**	Nr of accounts barred **None at this time.**	Nr of domains barred **7**
Data				
Measure 1.3	[insert wording if adapted]			
QRE 1.3.1 [insert wording if adapted]	**1. Advertisers are able to target/block site domains or apps at the campaign placement level.** **2. Advertisers are provided reporting on standard delivery metrics, primarily impression delivery, at a site domain and app level.** **3. Advertisers are automatically opted into Adobe Ad Cloud's "Global Blocklist" which includes reviewed sites and apps determined to violate policies or are determined to be inappropriate for advertising. This prevents ad delivery on those properties (1) unless the advertiser has manually opted out or (2) the advertiser has entered into a private deal exposed to or not transparent with these properties. Sites and Apps are reviewed for brand safety, invalid traffic, and ad placement.**			
Measure 1.4	[insert wording if adapted]			
QRE 1.4.1 [insert wording if adapted]	Outline relevant actions [suggested character limit: 2000 characters]			
Measure 1.5	[insert wording if adapted]			
QRE 1.5.1 [insert wording if adapted]	Outline relevant actions [suggested character limit: 2000 characters]			
QRE 1.5.2 [insert wording if adapted]	Outline relevant actions [suggested character limit: 2000 characters]			
Measure 1.5	Outline relevant actions [suggested character limit: 2000 characters]			
QRE 1.5.1 [insert wording if adapted]	Outline relevant actions [suggested character limit: 2000 characters]			
QRE 1.5.2 [insert wording if adapted]	Outline relevant actions [suggested character limit: 2000 characters]			
Measure 1.6	[insert wording if adapted]			
QRE 1.6.1 [insert wording if adapted]	**Adobe Ad Cloud offers several 3rd Party brand-safety targeting services that can be applied to campaign placements through our partners, with a fee. Pre-bid services halt impression delivery at the app, site or page level. These services are optional.**			

QRE 1.6.2 [insert wording if adapted]	Outline relevant actions [suggested character limit: 2000 characters]
QRE 1.6.3 [insert wording if adapted]	Outline relevant actions [suggested character limit: 2000 characters]
QRE 1.6.4 [insert wording if adapted]	Outline relevant actions [suggested character limit: 2000 characters]
SLI 1.6.1 [change wording if adapted]	Methodology of data measurement [suggested character limit: 500 characters]
	In view of steps taken to integrate brand safety tools: % of advertising/ media investment protected by such tools:
Data	

II. Scrutiny of Ad Placements				
Commitment 2 Relevant Signatories participating in advertising commit to prevent the misuse of advertising systems to disseminate Disinformation in the form of advertising messages. [change wording if adapted]				
Measure 2.1	[insert wording if adapted]			
QRE 2.1.1 [insert wording if adapted]	**Adobe Advertising Clouds advertising policy clearly states that false or misleading ads are prohibited. Additionally Political ads are prohibited.** **https://experienceleague.adobe.com/docs/advertising-cloud/policies/ad-requirements-policy.html?lang=en**			
SLI 2.1.1 – Numbers by actions enforcing policies above [change wording if adapted]	**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 remove the ad and review Adobe's Ads Requirements Policy. If three separate event violations are found from the same advertiser, they will be removed from the platform.**			
	No advertisers have been found to violate Adobe Advertising Cloud's advertising policy regarding	Type of Action 2 [linked to the policy mentioned in QRE]	Type of Action 3 [linked to the policy mentioned in QRE]	Type of Action 4 [linked to the policy mentioned in QRE]

	disinformation or misinformation.			
Data				
Measure 2.2	[insert wording if adapted]			
QRE 2.2.1 [insert wording if adapted]	**Adobe Advertising Cloud is assessing services available from current and new partners for disinformation or misinformation. This includes block lists, measurement or reporting, and pre-bid services.**			
Measure 2.3	[insert wording if adapted]			
QRE 2.3.1 [insert wording if adapted]	Outline relevant actions [suggested character limit: 2000 characters] **Ads are scanned by 3rd party partner to determine category.** **Ads from categories that pertain to Adobe Advertising Cloud's advertising policy are flagged and reviewed for material that violates Adobe Advertising Cloud's advertising policy.**			
SLI 2.3.1 [change wording if adapted]	Methodology of data measurement [suggested character limit: 500 characters]			
	Number of ads removed (as well as reach of ads before they were successfully removed) **No ads were removed for violations of Adobe Advertising Cloud's advertising policy related to disinformation or misinformation.**		Number of ads prohibited	
Data				
Measure 2.4	[insert wording if adapted]			
QRE 2.4.1 [insert wording if adapted]	**If an advertiser is found to violate Adobe's Ads Requirements Policy, they are notified via email. This notice includes the specific ad in violation, the policy it violates, and a link to Adobe's Ads Requirements Policy. They are also notified that three violations may result in removal from the platform. Advertisers can appeal this process and be subject to a 90 days grace period to be reviewed if any additional violations are levied against them. The strikes may be removed after these conditions are met.**			
SLI 2.4.1 [change wording if adapted]	Methodology of data measurement [suggested character limit: 500 characters]			
	Number of appeals 0		Proportion of appeals that led to a change of the initial decision	
Data				

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 multiple third-party providers offering misinformation and disinformation review of third party sites and apps. These providers 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 7 domains found on publicly available reports to begin to demonetize distributors of dis/misinformation.**

IV. Integrity of Services	
Commitment 15 Relevant Signatories that develop or operate AI systems and that disseminate AI-generated and manipulated content through their services (e.g. deep fakes) commit to take into consideration the transparency obligations and the list of manipulative practices prohibited under the proposal for Artificial Intelligence Act. [change wording if adapted]	
Measure 15.1	[insert wording if adapted]
QRE 15.1.1 [insert wording if adapted]	**Adobe supported the development and launch of Content Credentials, which act like a nutrition label for digital content and is fast becoming an industry standard. The user-directed Content Credentials allow creators to provide attribution for their work. In the context of generative AI, Content Credentials can indicate whether a digital file was human-created, AI-edited, or AI-generated, allowing viewers to decide for themselves whether to trust it. Adobe automatically attaches Content Credentials to Adobe Firefly generations to indicate that generative AI was used in the creation process.**

	This information enhances transparency for their audience.
Measure 15.2	[insert wording if adapted]
QRE 15.2.1 [insert wording if adapted]	Outline relevant actions [suggested character limit: 2000 characters]

V. Empowering Users				
Commitment 17 In light of the European Commission's initiatives in the area of media literacy, including the new Digital Education Action Plan, Relevant Signatories commit to continue and strengthen their efforts in the area of media literacy and critical thinking, also with the aim to include vulnerable groups. [change wording if adapted]				
Measure 17.1	[insert wording if adapted]			
QRE 17.1.1 [insert wording if adapted]	https://contentauthenticity.org/media-literacy **The Adobe-led CAI has also invested in creating and promoting media literacy curricula to educate the public about the dangers of deepfakes and tools available today to help them determine what's true online. In partnership with the Adobe Education team, the CAI updated our media literacy curriculum in February 2024 to include Generative AI curricular materials.** **These standards-aligned lessons introduce students to generative AI and engage them in critical conversations surrounding the technology.**			
SLI 17.1.1 - actions enforcing policies above [change wording if adapted]	Methodology of data measurement [suggested character limit: 500 characters]			
	Total count of the tool's impressions	Interactions/ engagement with the tool	Other relevant metrics	Other relevant metrics
Data				
Measure 17.2	[insert wording if adapted]			
QRE 17.2.1 [insert wording if adapted]	Outline relevant actions [suggested character limit: 2000 characters]			
	Methodology of data measurement [suggested character limit: 500 characters]			

SLI 17.2.1 - actions enforcing policies above [change wording if adapted]	Nr of media literacy/ awareness raising activities organised/ participated in	Reach of campaigns	Nr of participants	Nr of interactions with online assets	Nr of participants (etc)
Data					
Measure 17.3	[insert wording if adapted]				
QRE 17.3.1 [insert wording if adapted]	Outline relevant actions [suggested character limit: 2000 characters]				

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	**C2PA standard and Content Credentials**
QRE 20.1.1 [insert wording if adapted]	**Adobe is a co-founder and steering committee member of the standards organisation, the Coalition for Content Provenance and Authenticity (C2PA), a Joint Development Foundation project within the Linux Foundation. Adobe co-chairs the steering committee which meets weekly, chairs the Technical Working Group and has representatives on the User Experience Task Force, Threats and Harms Task Force. The C2PA also receives support from Adobe employees in Communications and Policy for C2PA external engagement.** **We are committed to working with other C2PA members such as Microsoft, BBC, Intel, Google (joined in 2024), Sony and TruePic to ensure open technical standards for provenance are maintained to the highest standards; used to develop and implement content provenance across the ecosystem which is interoperable; and ultimately adopted by international standards organisations as the gold standard for helping to combat misinformation.** **Internally, at Adobe we also have a team of full-time employees, dedicated to working on provenance. This includes engineers helping to develop and maintain our open-source tooling for the community, user-experience designers, and a team dedicated to advocacy and education, supporting adoption, and growing the community globally.**

	In popular Adobe creative tools including Photoshop and Lightroom, consumers have access to Content Credentials, free, open-source technology leveraging the C2PA open technical standard that serves as a "digital nutrition label" for content. Content Credentials can include important information which may include the creator's name, the date an image was created, what tools were used to create an image and any edits that were made along the way, **Other applications in Adobe Creative Cloud including Illustrator, Adobe Express, Adobe Stock, and Behance also support Content Credentials, and Adobe is continuing to roll out capabilities across products.** **Additionally, Adobe automatically attaches a Content Credential to content created with Adobe Firefly that indicates that generative AI was used in the creation process. This level of transparency allows customers to see content with context and helps build a more trustworthy digital space.**
Measure 20.2	**Enabling industry adoption of Content Credentials**
QRE 20.2.1 [insert wording if adapted]	**Google joined the C2PA steering committee in February 2024 and is actively exploring how to incorporate Content Credentials into its own products and services in the future.** **In January 2024, OpenAI announced details around its initiatives to protect the integrity of global elections, including support the C2PA standard and Content Credentials for images generated by DALL·E 3, which is now available and then support in its new voice to video offering Sora.** **In February 2024, Meta announced updates to its standard for labeling AI-generated images, ahead of global elections this year – which includes its plan to build on the C2PA's industry standard solution for adding provenance to content to ensure that people have transparency around the content they see online.** **Microsoft has brought Content Credentials to all AI-generated images created with Bing Image Creator. The invisible digital watermark feature adheres to C2PA specifications and confirms the time and date of original creation. Microsoft will also integrate Content Credentials into Microsoft Designer.** **Qualcomm's latest Snapdragon8 Gen3 platform's camera system works with Truepic to support Content Credentials that empower authenticity of photo and video across smartphones.** **Leica launched the world's first camera with Content Credentials built-in – delivering authenticity at the po capture.**

	Sony will incorporate Content Credentials based global C2PA standard format into their new line of cameras and future firmware updates. This capability will be available Spring 2024 in the new Alpha 9 III and Sony's Alpha 1 and Alpha 7S III models via firmware updates. **Nikon is bringing Content Credentials to future camera models.** **Publicis Groupe is adopting Content Credentials for creative and client work for consumer campaigns.**

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]	**Adobe has participated in the Taskforce Plenary meetings. In addition, Adobe is an active member of the GenAI subgroup and has participated in the virtual meetings of the subgroup.**

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 overseen by the General Counsel.**
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]

Reporting on the service’s response during an election

Reporting on the service's response during an election	
European Elections	
Threats observed or anticipated at time of reporting: AI-generated or AI-manipulated audio, video, and images that deceptively fake or alter the appearance, voice, or actions of political candidates, election officials, and other key stakeholders in a democratic election, or that provide false information to voters about when, where, and how they can vote.	
Mitigations in place – or planned - at time of reporting: [suggested character limit: 2000 characters].	
[Note: Signatories are requested to provide information relevant to their particular response to the threats and challenges they observed on their service(s). They ensure that the information below provides an accurate and complete report of their relevant actions. As operational responses to crisis/election situations can vary from service to service, an absence of information should not be considered a priori a shortfall in the way a particular service has responded. Impact metrics are accurate to the best of signatories' abilities to measure them].	
Empowering Users	
Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.	
Specific Action applied (with reference to the Code's relevant Commitment and Measure)	**At the Munich Security Conference in February 2024, Adobe together with 19 other leading technology companies, pledged to help prevent deceptive AI content from interfering with this year's global elections.** **The "Tech Accord to Combat Deceptive Use of AI in 2024 Elections" is a set of commitments to deploy technology countering harmful AI-generated content meant to deceive voters. Signatories pledge to work collaboratively on tools to detect and address online distribution of such AI content, drive educational campaigns, and provide transparency, among other concrete steps. It also includes a broad set of principles, including the importance of tracking the origin of deceptive election-related content and the need to raise public awareness about the problem.** **Digital content addressed by the accord consists of AI-generated audio, video, and images that deceptively fake or alter the appearance, voice, or actions of political candidates, election officials, and other key stakeholders in a democratic election, or that provide false information to voters about when, where, and how they can vote.** **"Attaching provenance signals to identify the origin of content where appropriate and technically feasible" is one of the accord´s principle goals and the signatories commit to taking the following steps through 2024 with regard to provenance:** **Developing and implementing technology to mitigate risks related to Deceptive AI Election content by:**

	a. Supporting the development of technological innovations to mitigate risks arising from Deceptive AI Election Content by identifying realistic AI-generated images and/or certifying the authenticity of content and its origin, with the understanding that all such solutions have limitations. This work could include but is not limited to developing classifiers or robust provenance methods like watermarking or signed metadata (e.g. the standard developed by C2PA or SynthID watermarking). **b. Continuing to invest in advancing new provenance technology innovations for audio video, and images.** **c. Working toward attaching machine-readable information, as appropriate, to realistic AI-generated audio, video, and image content that is generated by users with models in scope of this accord.**
	Indication of impact (at beginning of action: expected impact) including relevant metrics when available