# CMP Validator User Guide

**Introduction** **4**

**Installation** **4**

Chrome browser extension 4

Non-Web based CMPs 4

Requesting access to the Validator 4

Installing the extension 5

1. Sign in to Chrome 5

2. Add extension to Chrome 6

3. Allow extension to run in incognito mode 9

**Getting started** **12**

Sites that do not have a CMP that supports the TCF 14

**Using the CMP Validator** **16**

Compliance Checks 16

Technical compliance checks 18

Policy compliance checks 19

CMP information 20

CMP API 20

CMP API - ping 20

CMP API - getConsentData 21

CMP API - getVendorConsents 21

CMP API - getPublisherConsents (optional) 21

CMP API - getVendorList (optional) 21

pubvendors.json (optional) 21

Consent string data 22

Consent strings 22

Cookies 24

Purposes 25

Vendors 26

Publisher standard purpose consents 26
Publisher custom purpose consents 27
Tags that contain the consent string 27
Summary - tags that contain the consent string 27
No consent string found 28
Information with no value 28
CSV Results 29
Save to CSV 29
Download CSV 29
Clear CSV Results 29

**Testing a site using 'incognito' mode 30**

**I'm a CMP, what do I have to do? 32**
Run the Validator on a site where your CMP is installed 32
Go through each of the manual checks 33
Send CSV results to IAB Europe 34
Resolve any issues found within 30 days 34

**Frequently asked questions 35**
What is the IAB Europe CMP Validator (the Validator)? 35
Why was the Validator developed? 35
Who developed the Validator? 35
What was involved in the development of the Validator? Has it been tested in market? 35
Where can I find the CMP Validator and how do I install it? Who can use the Validator? 36
What operating systems are compatible with the Validator? 36
Does the Validator run on mobile devices? 36
I have a non-Web based CMP, can I use the Validator? 36
How will the Validator be used in market? 36
Who verifies the operational compliance of the test? 37
What is the validation process for existing CMPs? 37
What is the validation process for new CMPs? 37
Will all Validator testing be managed by CMPs on a self-assignment basis? 37
If a CMP does not pass the validation tool operational requirements, what will be the next steps? 37
Who will be informed if a CMP does not comply in the given timeframe? 37

Will the MO make public the results of the testing? 38
What does the MO hope to achieve through the implementation of the Validator? 38
Is it likely that the Validator will accelerate CMP deactivations? What will be the impact on the TCF? 38
Is the Validator able to test for both TCF version 1 and TCF version 2 operational compliance? 39
If a complaint is raised with a DPA about a CMP registered with the TCF, what is the process? 39
What is the deactivation process? 39
What is the enforcement process? 39
How do I get the latest version of the Validator? 39
When will the Validator support TCF version 2? 40

***Note: all screenshots contained in this document are for illustrative purposes only.***

# Introduction

The IAB Europe CMP Validator (Validator) is a tool that helps Consent Management Providers (CMPs) and publishers check their compliance with the IAB Europe Transparency & Consent Framework (TCF) Technical Specifications and Policy.

# Installation

## Chrome browser extension

The Validator is a Chrome extension. This enables the tool to analyse live CMP installations on any site. The extension can be used in the Windows or macOS versions of Chrome. It is not possible to add an extension to mobile or tablet browsers.

## Non-Web based CMPs

If you have an in-app or non-Web based CMP you will not be able to use the Validator - please submit the appropriate form below as part of the compliance process instead of using the Validator:

- V1.1 non-Web based CMP form
- V2.0 non-Web based CMP form

## Requesting access to the Validator

The Validator has been published to the Chrome Web Store in private mode. This means it does not appear in searches and is only available to authorised users.

Only CMPs registered with the Transparency & Consent Framework (TCF), or publishers running an IAB TCF registered CMP, are authorised to use the tool.

A Gmail account is required to use the tool. To request access, please send an email **from your organisation's domain** to: tcf.compliance@iabeurope.eu, with details of the Gmail account you wish to use.

# Installing the extension

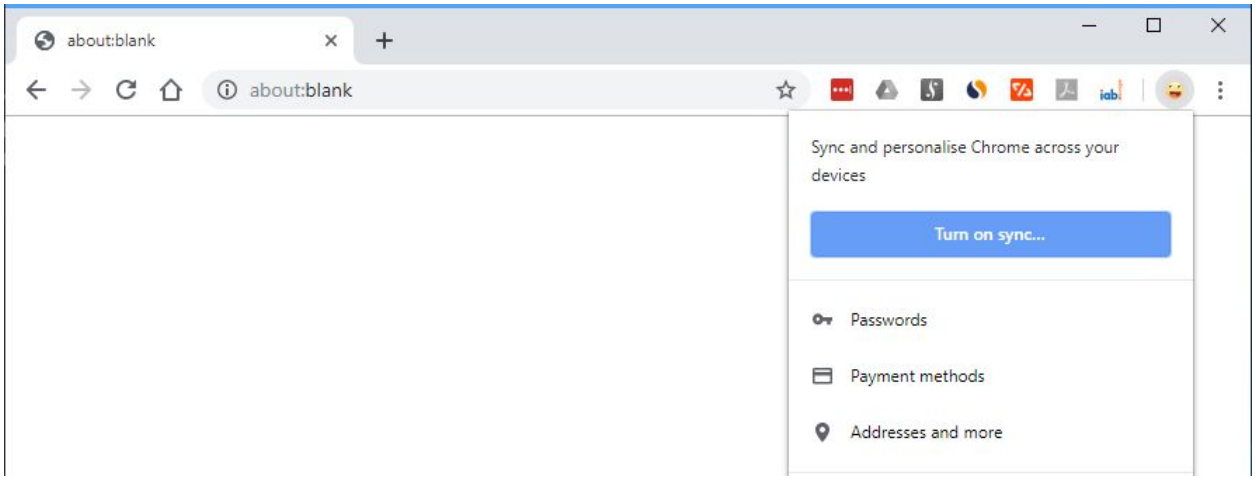
Once IAB Europe has confirmed that your Gmail account has been authorised to use the tool, follow these steps to enable the extension in Chrome:

1. Sign in to Chrome
2. Add extension to Chrome
3. Allow extension to run in incognito mode

## 1. Sign in to Chrome

You must be signed in to Chrome with the Gmail account you sent us to install the extension.

You can sign in using the icon next to the settings in the top right hand corner of the browser. Note that the icon on your browser will be different to the one shown below.



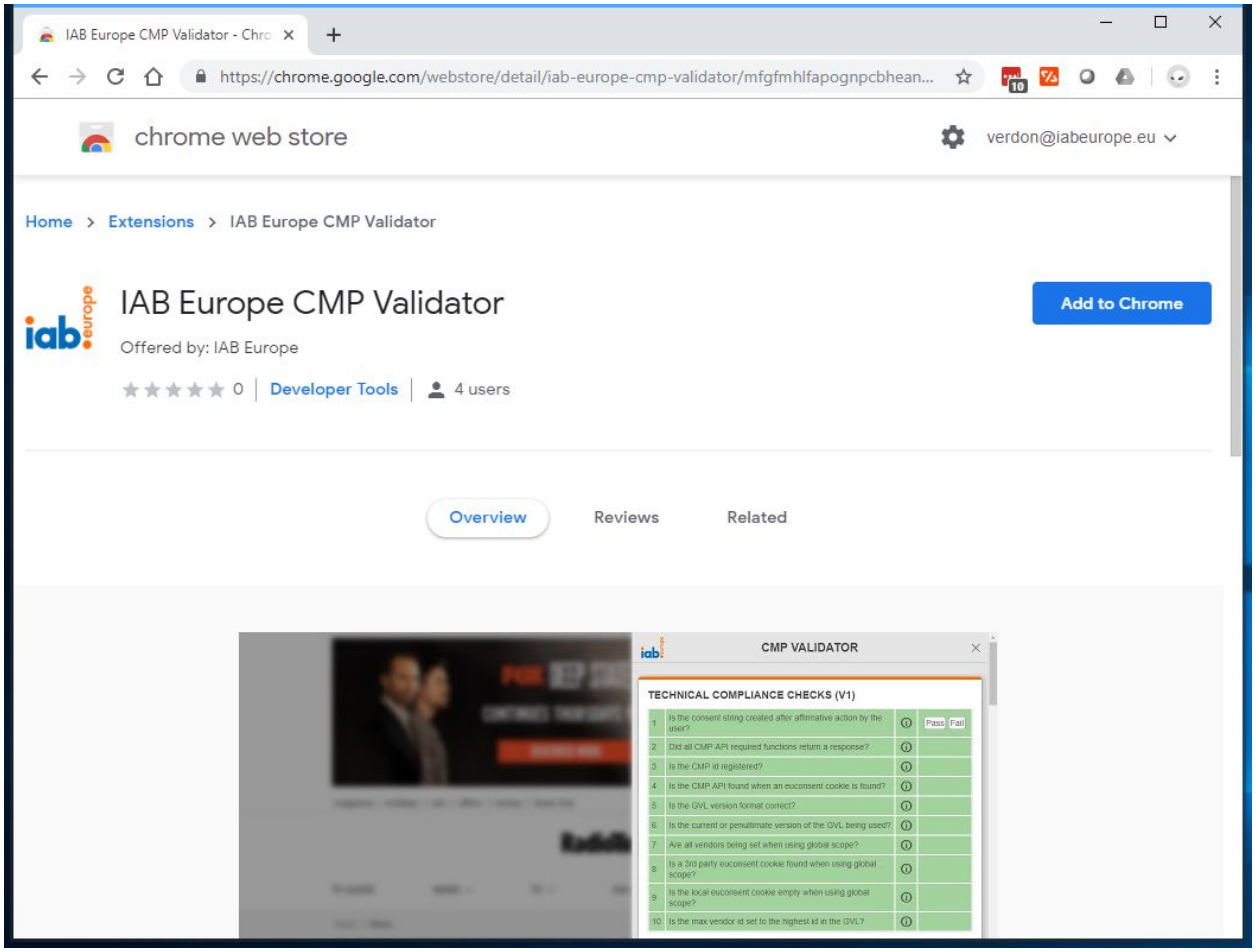
## 2. Add extension to Chrome

Use this link to view the extension in the Chrome Web Store

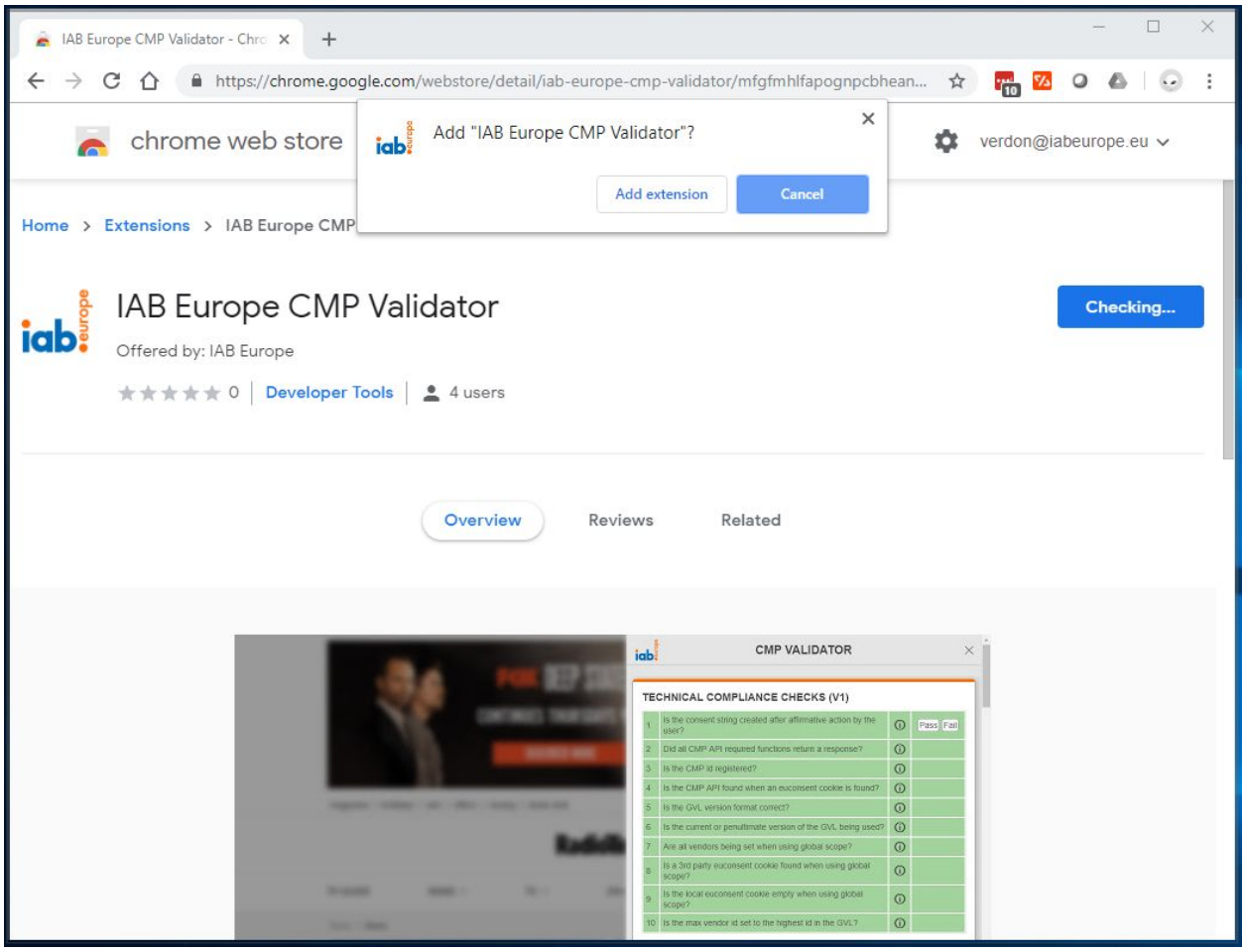
https://chrome.google.com/webstore/detail/iab-europe-cmp-validator/mfgfmhlfapognpcbheanamlejcejcebc?authuser=1

Now click the ‘Add to Chrome’ button.

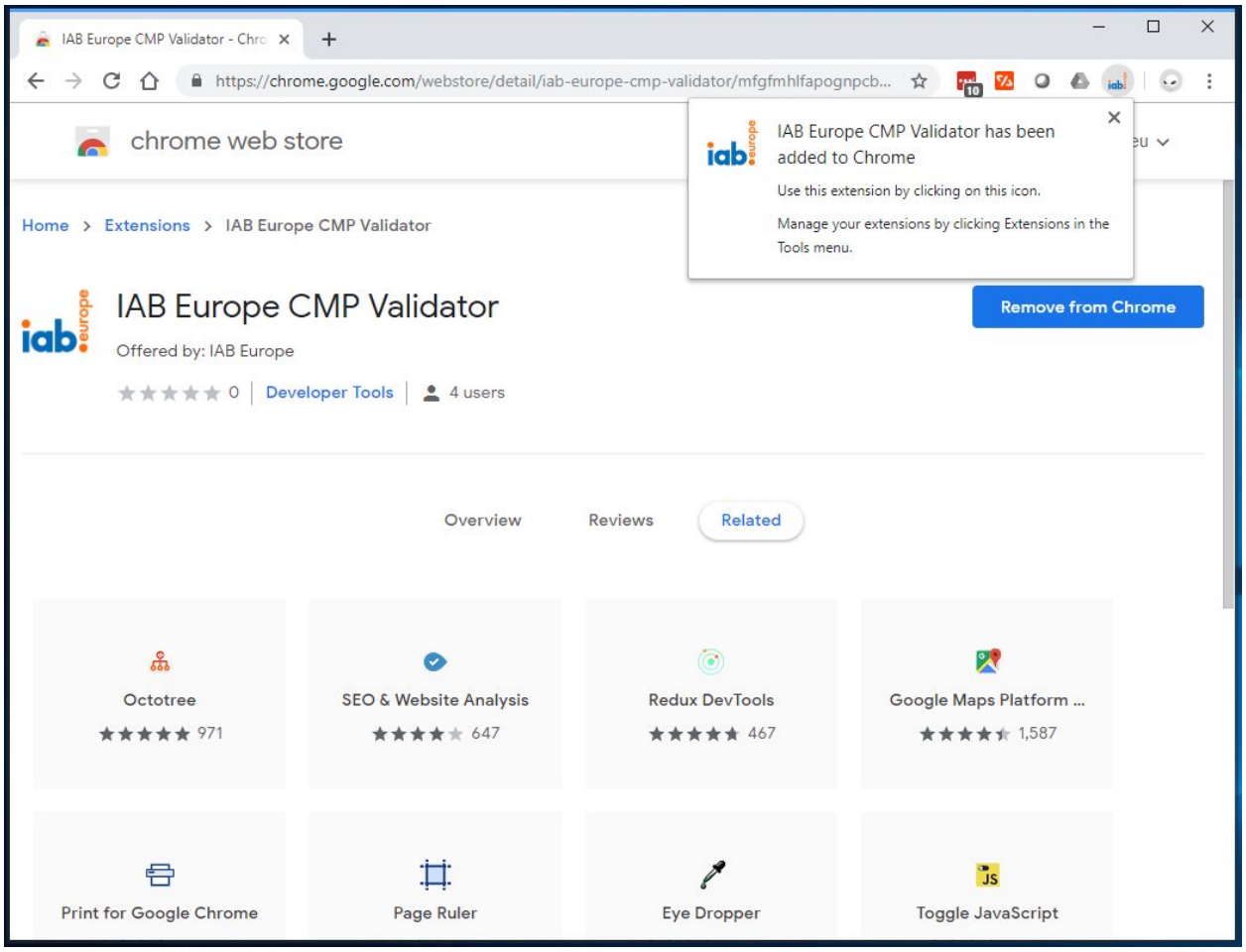
***Note: if you get a ‘404’ error when accessing this URL it means your Gmail account is not yet authorised to use the tool. Try again in an hour.***



Confirm you want to add the extension by clicking ‘Add extension’.



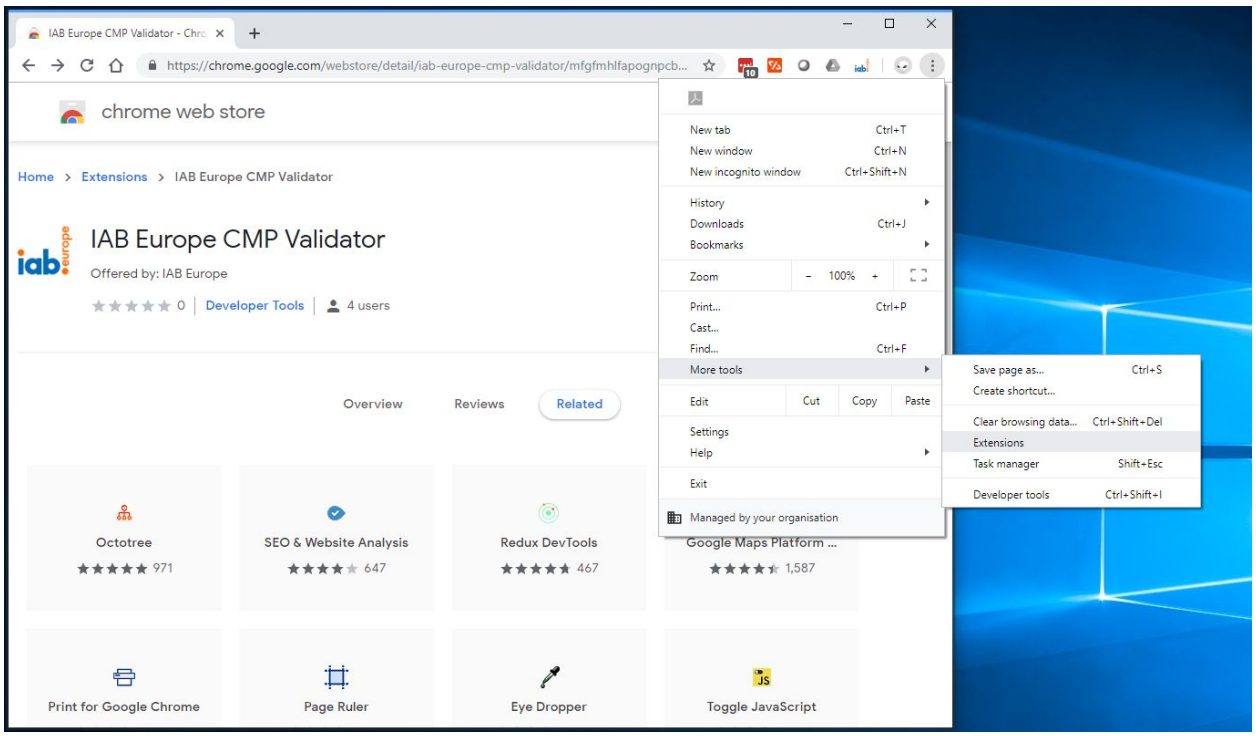
Chrome will then confirm that the extension has been added.



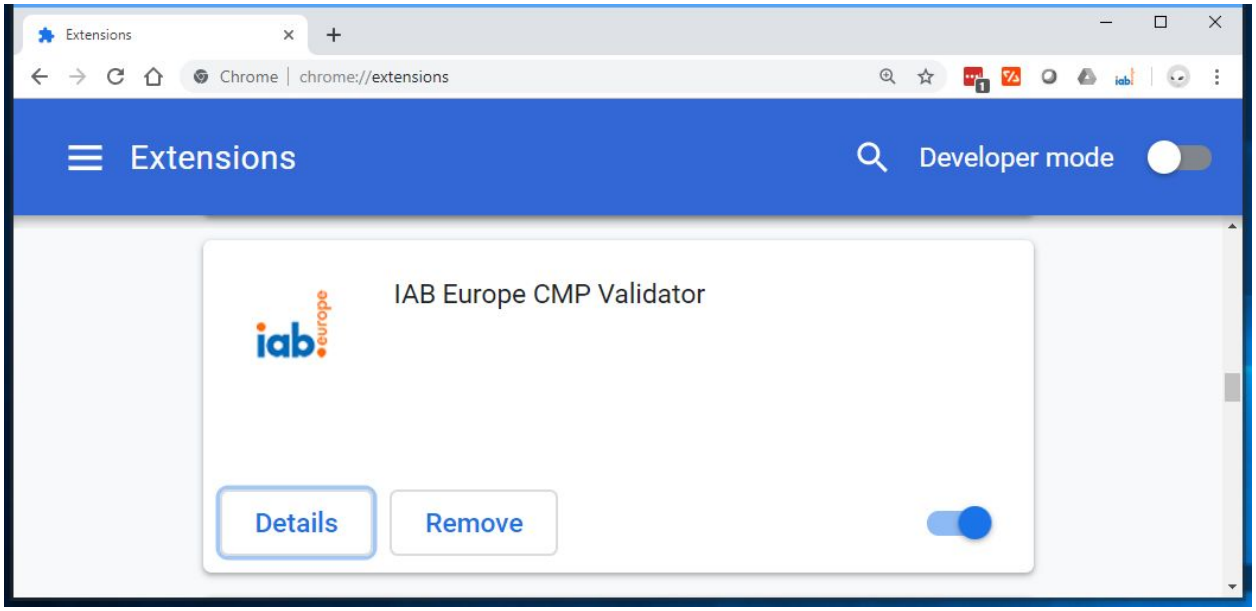
## 3. Allow extension to run in incognito mode

Some of the tests need to be run using Chrome's incognito mode. Follow these steps to allow the extension to run when you launch an incognito browser window.

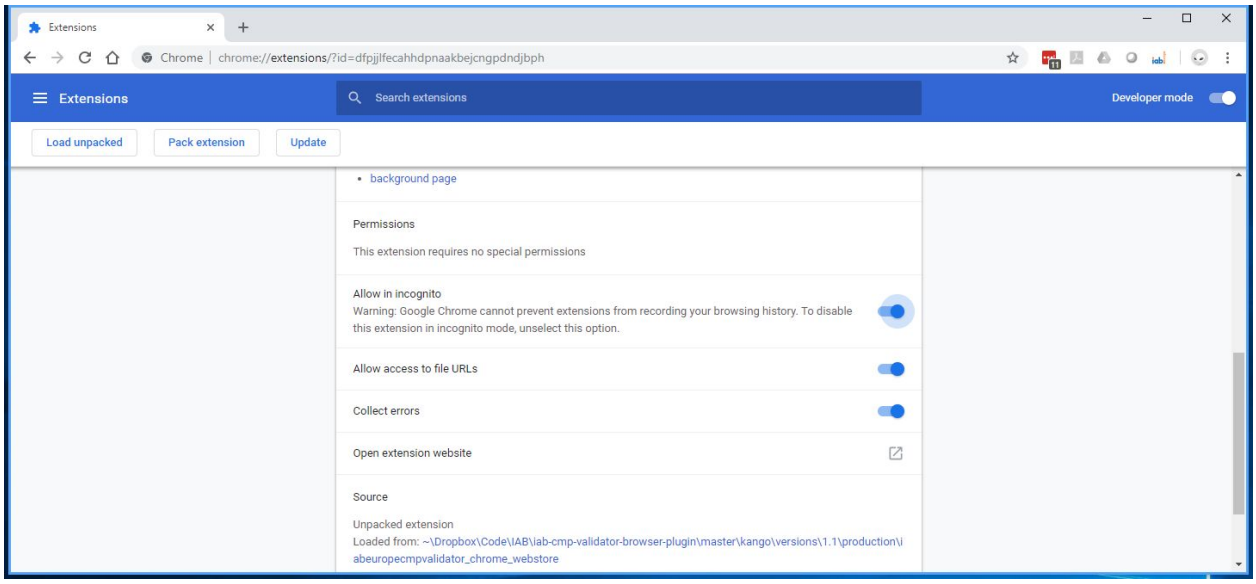
**Go to Settings > More tools > Extensions**



Find the IAB Europe CMP Validator extension and click on ‘Details’.



Now toggle the ‘Allow in incognito’ option.

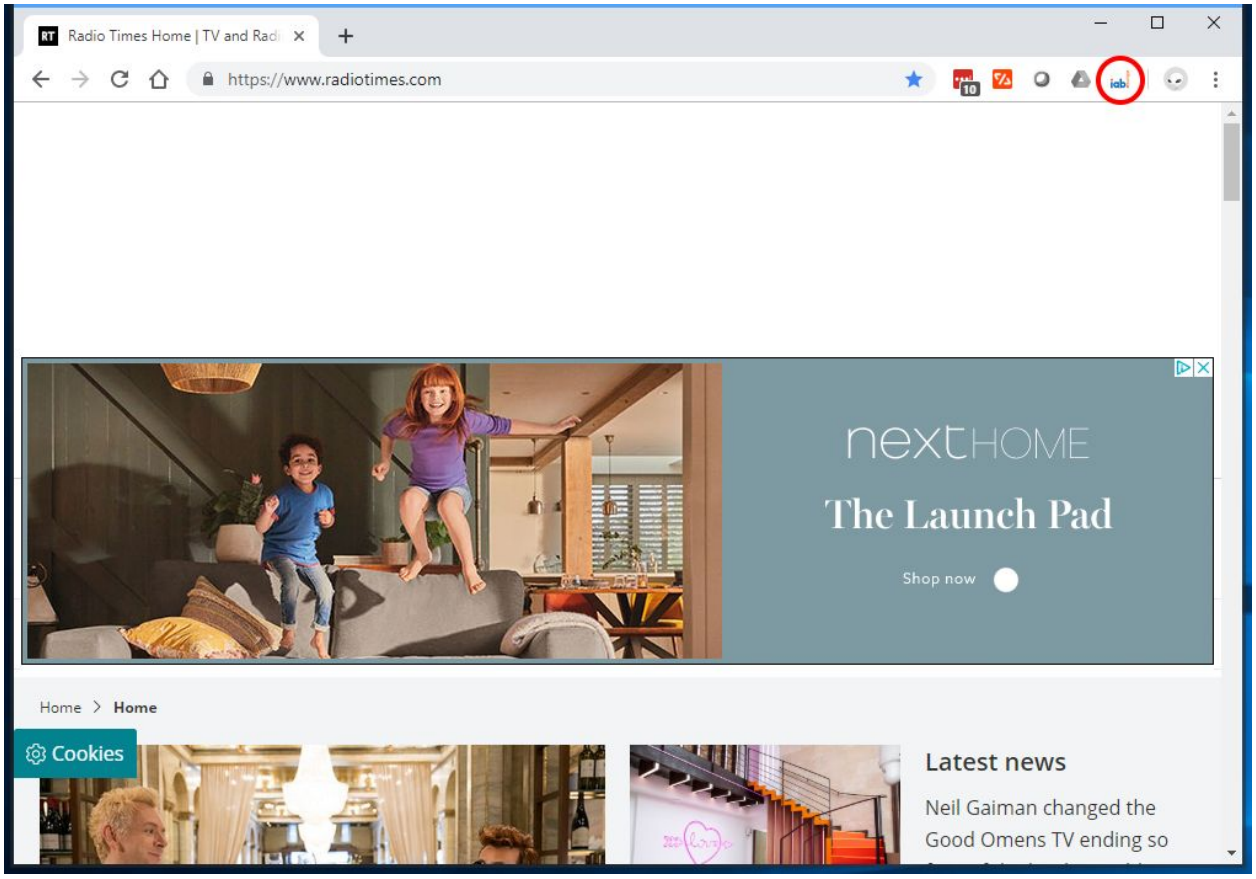



That’s it, you’re done!

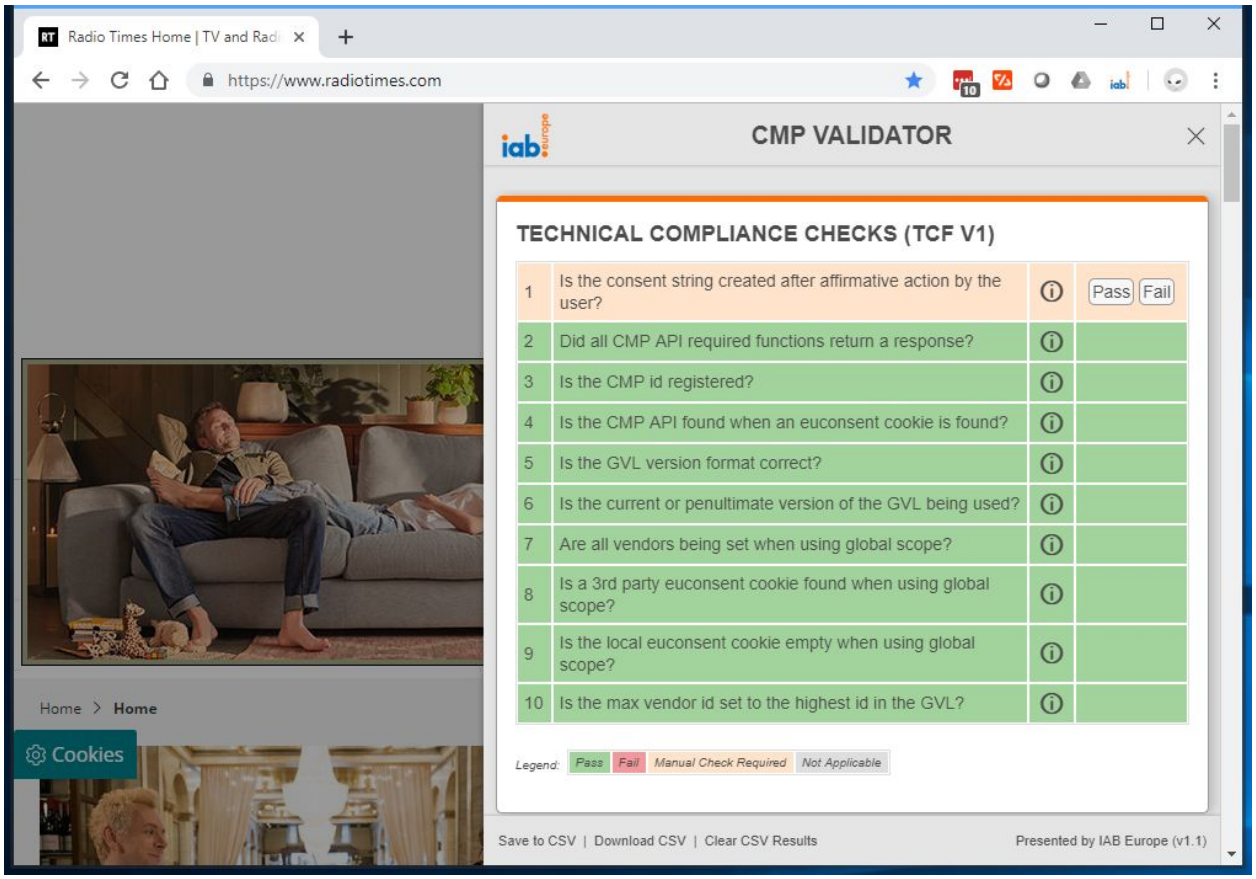
# Getting started

Once installed, you can browse to any Website and click the icon in the top bar to run the CMP Validator.

The tool works by adding code into the actual Website being viewed. Note that on sites that load many 3rd party scripts, it can take a few seconds for the CMP Validator scripts to run.



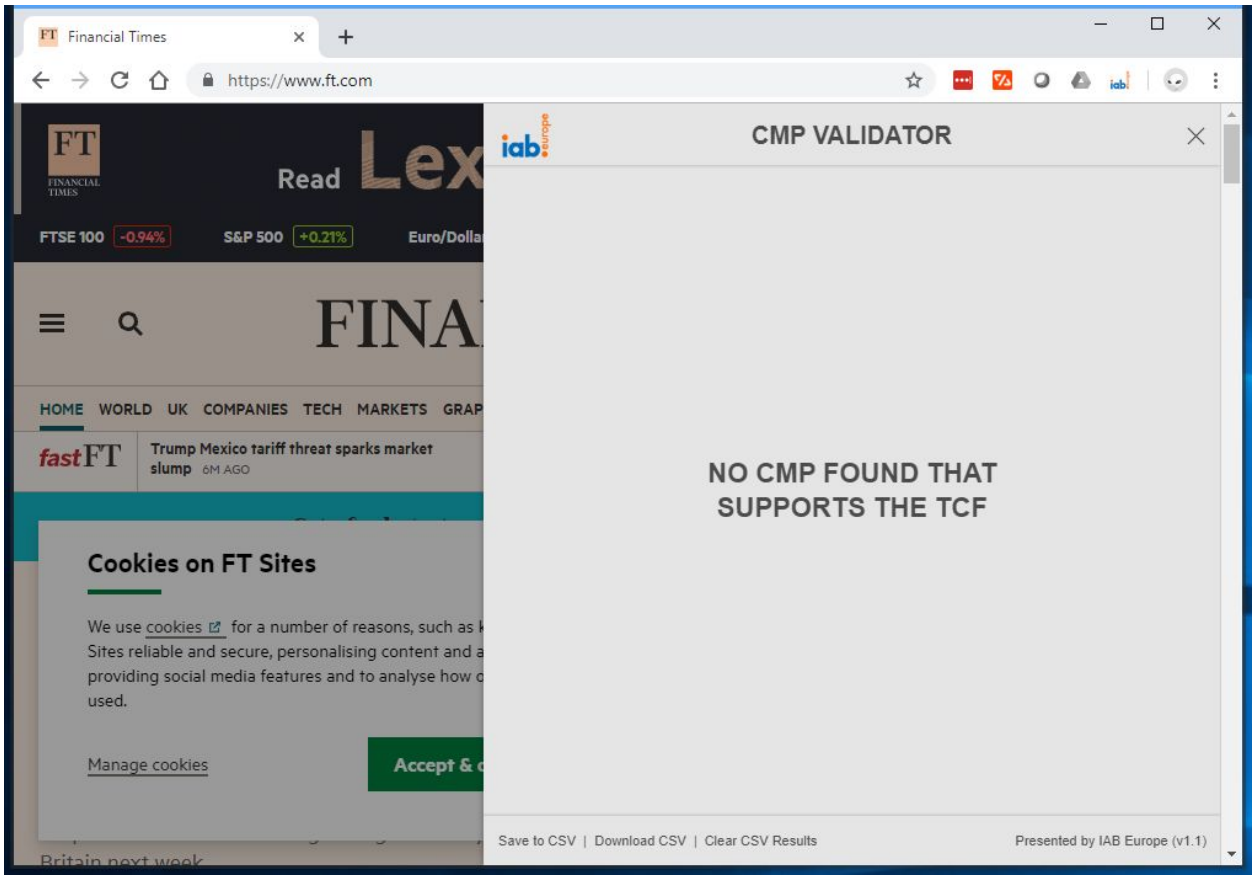
Clicking the icon in the top bar will activate the CMP Validator which will appear as a slider that overlays the site.



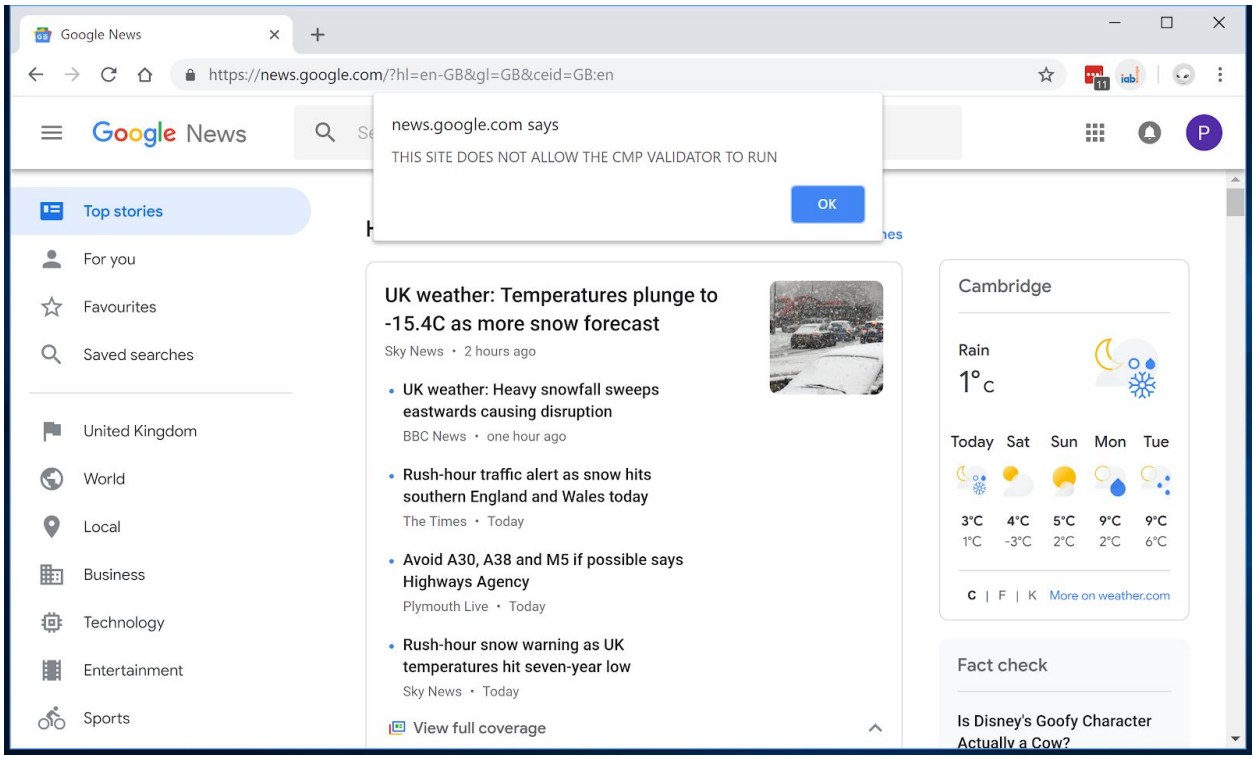

You can dismiss the CMP Validator by clicking on the icon again, using the ‘X’ in the top right corner or clicking outside of the CMP Validator user interface.

## Sites that do not have a CMP that supports the TCF

If you run the CMP Validator on a site that does not have a CMP that supports the TCF you will see the following message.



Some sites implement a Content Security Policy that prevents unknown scripts from running on the page - in these cases the CMP Validator is not able to run and the following message will be shown.




***Note: only a couple of sites have been found where the CMP Validator could not run, out of 100s tested.***

# Using the CMP Validator

The Validator has three key feature areas:

1. Compliance checks
2. CMP information
3. CSV results

## Compliance Checks

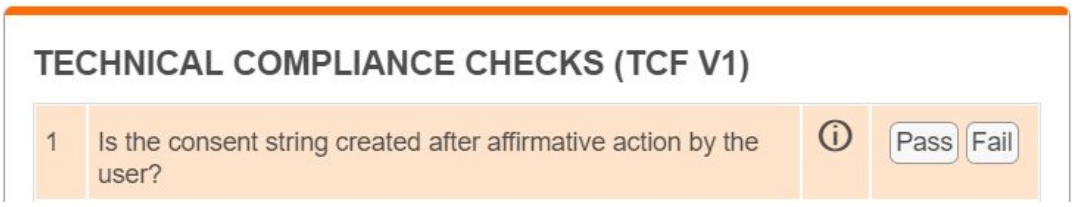
The compliance checks are split into two sections:

- Technical compliance checks
- Policy compliance checks

Each check is colour coded according to four possible states:

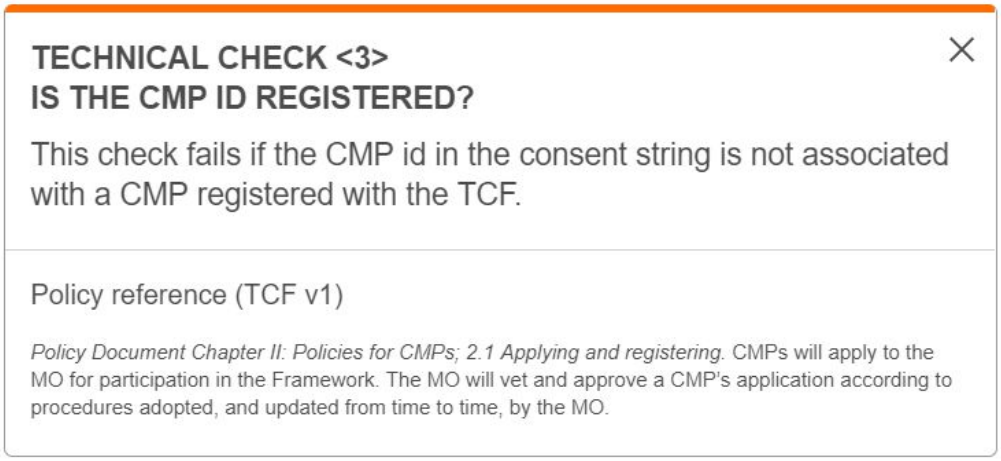
- Pass - the check has passed
- Fail - the check has failed
- Manual check required - this check must be run manually
- Not applicable - not relevant for this installation

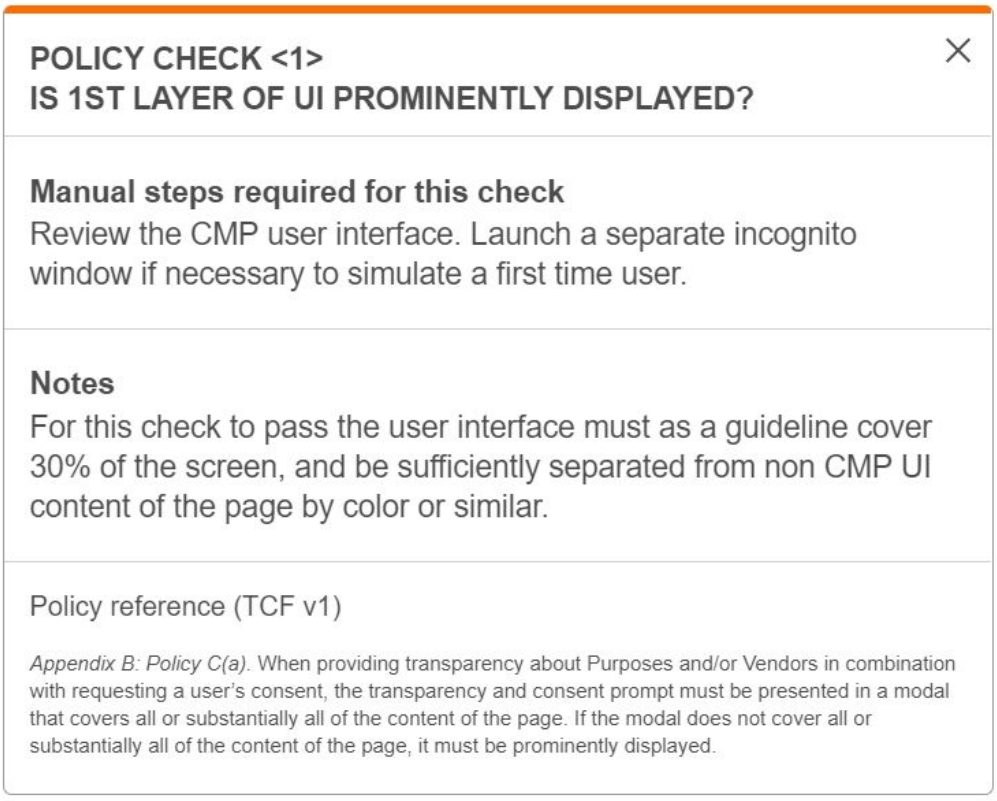
The language of each check has been written as a self-explanatory question.




If the answer to the question is ‘yes’ the check has passed, if the answer to the question is ‘no’, the check has failed.

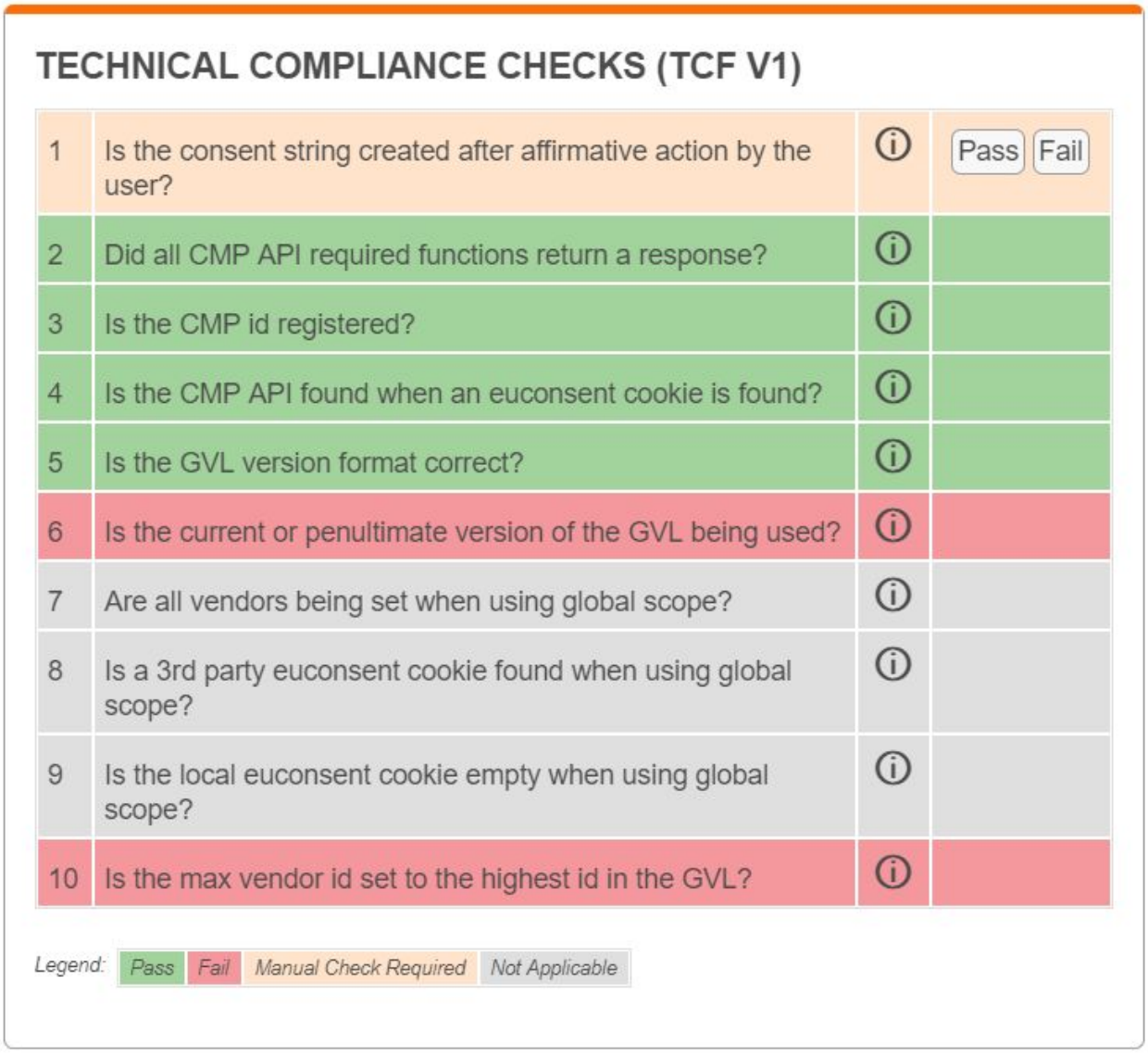
Each check also has an info icon (i) that shows more information, which includes a) failure state details; b) manual steps; c) additional notes and d) the policy reference.



## Technical compliance checks

These are checks regarding technical implementation. Most of the technical checks are run automatically.



TECHNICAL COMPLIANCE CHECKS (TCF V1)

| | | | |
|---|---|---|---|
| 1 | Is the consent string created after affirmative action by the user? | ⓘ | Pass Fail |
| 2 | Did all CMP API required functions return a response? | ⓘ | |
| 3 | Is the CMP id registered? | ⓘ | |
| 4 | Is the CMP API found when an euconsent cookie is found? | ⓘ | |
| 5 | Is the GVL version format correct? | ⓘ | |
| 6 | Is the current or penultimate version of the GVL being used? | ⓘ | |
| 7 | Are all vendors being set when using global scope? | ⓘ | |
| 8 | Is a 3rd party euconsent cookie found when using global scope? | ⓘ | |
| 9 | Is the local euconsent cookie empty when using global scope? | ⓘ | |
| 10 | Is the max vendor id set to the highest id in the GVL? | ⓘ | |

Legend: Pass Fail Manual Check Required Not Applicable

## Policy compliance checks

These are policy related checks that cannot be run automatically and require a human to review the user interface to determine if the check passes or fails.

### POLICY COMPLIANCE CHECKS (TCF V1)

| | | | |
|---|---|---|---|
| 1 | Is 1st layer of UI prominently displayed? | ⓘ | Pass Fail |
| 2 | Are all Purposes shown in the 1st layer of the user interface? | ⓘ | Pass Fail |
| 3 | Is a link to Vendors provided in the 1st layer of the user interface? | ⓘ | Pass Fail |
| 4 | Are calls to action of equal visual prominence? | ⓘ | Pass Fail |
| 5 | Is the user informed of their right to withdraw consent at any time in the 1st layer and how to do so? | ⓘ | Pass Fail |
| 6 | Are the consequences of consenting or not consenting explained in the 1st layer? | ⓘ | Pass Fail |
| 7 | Is the user informed that access to information on their device is taking place by third parties in the 1st layer? | ⓘ | Pass Fail |
| 8 | Is the user informed that their personal data is processed by third parties in the 1st layer, with examples of such data? | ⓘ | Pass Fail |

## CMP information

This section shows all the information that has been retrieved about the CMP running on the site. The section heading shows the name of the CMP if it has been identified.

### CAPTIFY TECHNOLOGIES LIMITED

***CMP information***

| | |
|---|---|
| CMP id | 29 |
| CMP is a service | yes |
| TCF version | 1 |

### CMP API

Indicates whether the CMP API was found.

| | |
|---|---|
| __cmp found | yes |
| __cmpLocator iframe found | no |

### CMP API - ping

Details the response from the ping function.

| | |
|---|---|
| ping response | yes |
| cmpLoaded | yes |
| gdprAppliesGlobally | no |

## CMP API - getConsentData

Details the response from the getConsentData function.

| | |
|---|---|
| getConsentData response | yes |
| gdprApplies | yes |
| hasGlobalScope | no |

## CMP API - getVendorConsents

Indicates whether there was a response from the getVendorConsents function.

| | |
|---|---|
| getVendorConsents response | yes |

## CMP API - getPublisherConsents (optional)

Indicates whether there was a response from the optional getPublisherConsents function.

| | |
|---|---|
| getPublisherConsents response | no |

## CMP API - getVendorList (optional)

Indicates whether there was a response from the optional getVendorList function.

| | |
|---|---|
| getVendorList response | yes |

## pubvendors.json (optional)

Indicates whether a pubvendors.json file is available and if yes, provides a link to it.

| | |
|---|---|
| pubvendors.json exists | yes |

## Consent string data

This section shows information extracted from the consent string.

| | |
|---|---|
| CMP version | 2 |
| Consent string version | 1 |
| Vendor list version | 2 |
| Max vendor id | 612 |
| Consent screen | 0 |
| Consent language | en |

## Consent strings

When you run the CMP Validator it loads the consent strings found at that point in time.

The tool identifies all the consent strings available. It checks in three places: the CMP JS API, a local ‘euconsent’ cookie and a global ‘euconsent’ cookie.

The default consent string used by the publisher site is always shown first - if the consent string is available from the CMP JS API it is retrieved from there, if not, from the local cookie. The source of the default consent string is shown as either ‘via CMP JS API’ or ‘via local cookie’.

In order to understand how CMPs are working, it is possible to load **a different consent string**. This is especially useful to view the contents of the global consent string. The 'current' consent string being viewed and any that match it are always highlighted in green.

***Consent string - default (via CMP API getConsentData)***

BObI8LdOg2SVwAdACAENAC-AAAAmR7_____9____7_9uz_Gv_r_ff_3nW0739P1A_r_Oz_rm_-zzV44_lpQQRCEAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAAABAAAAACA

***Consent string - local cookie***

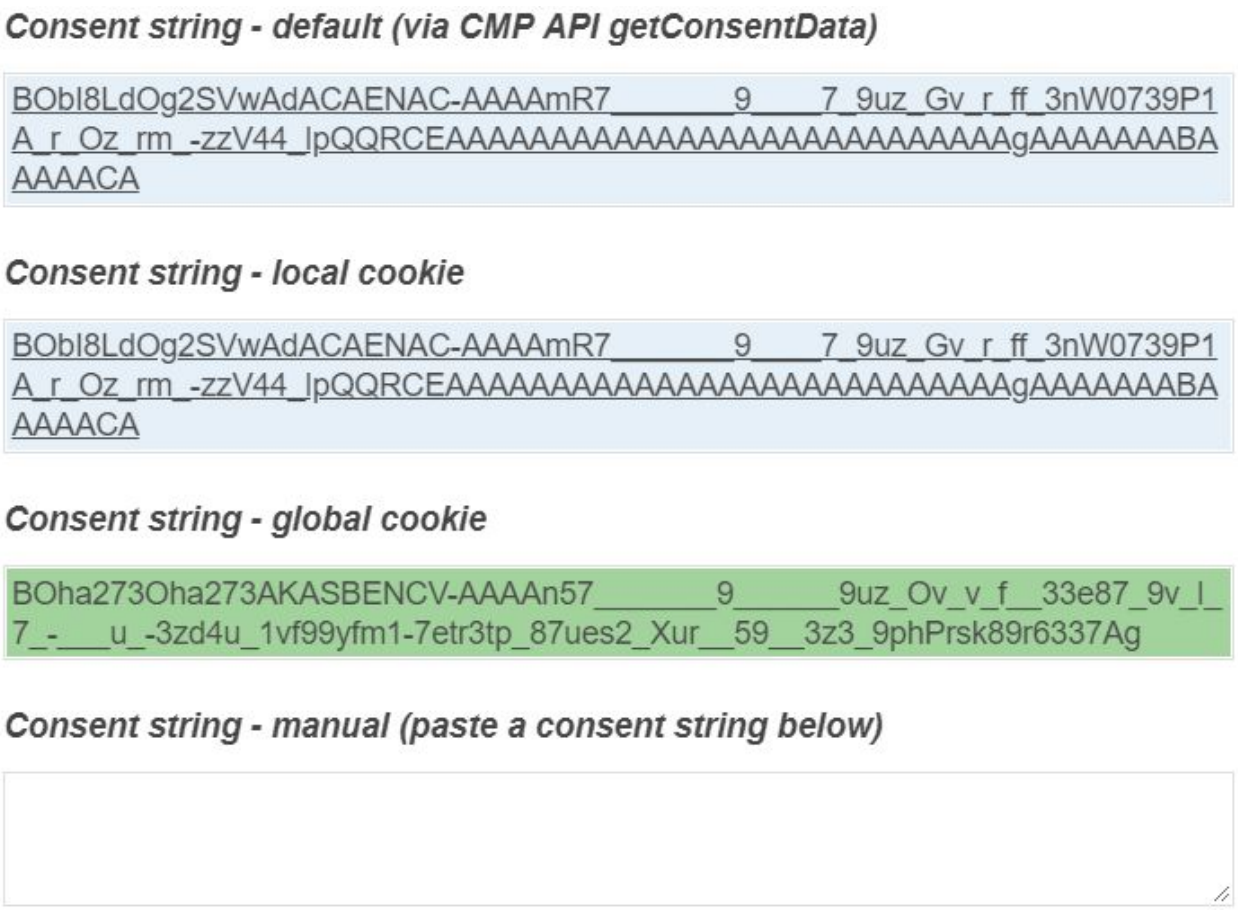
BObI8LdOg2SVwAdACAENAC-AAAAmR7_____9____7_9uz_Gv_r_ff_3nW0739P1A_r_Oz_rm_-zzV44_lpQQRCEAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAAABAAAAACA

***Consent string - global cookie***

BOha273Oha273AKASBENCV-AAAAn57_____9_____9uz_Ov_v_f__33e87_9v_l_7_-___u_-3zd4u_1vf99yfm1-7etr3tp_87ues2_Xur__59__3z3_9phPrsk89r6337Ag

Any consent string that is **different** to the current consent string being viewed is shown underlined which means you can click on it to load the contents of that consent string.

When clicking on a different consent string the CMP Validator will reload, showing the contents of the selected consent string. That consent string then becomes the 'current' consent string and is highlighted in green.




There is also a facility to paste in any consent string manually to see the contents of that string.

***Important note: compliance checks should be ignored when viewing a different consent string.***

## Cookies

The CMP Validator reports on the names of cookies which contain the ‘euconsent’ or ‘eupubconsent’ string.

| | |
|---|---|
| Local cookie names | eupubconsent |
| Global cookie names | euconsent |

## Purposes

The purposes allowed in the consent string are shown colour coded, green for ‘yes’, red for ‘no’. This makes it easy to change the purpose settings in the CMP user interface and check whether the consent string reflects those changes. The purpose id is shown in brackets next to the description.

*Purposes allowed*

| | |
|---|---|
| Information storage and access (1) | no |
| Personalisation (2) | no |
| Ad selection, delivery, reporting (3) | no |
| Content selection, delivery, reporting (4) | yes |
| Measurement (5) | yes |

## Vendors

The vendors allowed in the consent string are shown colour coded, green for ‘yes’, red for ‘no’. As above, this makes it easy to change the vendor settings in the CMP user interface and check whether the consent string reflects those changes. The vendor id is shown in brackets next to the name.

*Vendors*

| | |
|---|---|
| 1000mercis (388) | yes |
| 1020, Inc. dba Placecast and Ericsson Emodo (141) | no |
| 1plusX AG (92) | yes |
| 2KDirect, Inc. (dba iPromote) (217) | no |

## Publisher standard purpose consents

If set, the publisher’s standard purpose consents are shown here.

*Publisher standard purpose consents*

| | |
|---|---|
| 1 | yes |
| 2 | yes |
| 3 | yes |
| 4 | yes |
| 5 | yes |
| 6 | no |

## Publisher custom purpose consents

If set, the publisher's custom purpose consents will be shown here.

*Publisher custom purpose consents*

| |
|---|
| n/a |

## Tags that contain the consent string

Three sections at the bottom shows any <SCRIPT>, <IFRAME> or <IMG> tags in the page that contain the consent string.

| |
|---|
| https://s.cpx.to/fire.js?pid=12097&ref=&hn_ver=10&fid=f9371d9b-a87e-4b22-89a4-1db0c72e8e5f&gcv=BOha273Oha273AKASBENCV-AAAAn57_____9_____9uz_Ov_v_f__33e87_9v_l_7_-___u_-3zd4u_1vf99yfm1-7etr3tp_87ues2_Xur__59__3z3_9phPrsk89r6337Ag |
| https://ps.eyeota.net/pixel?pid=9c9gdbu&sid=26&t=ajs&cat=demand&c_b=1&gdpr=1&gdpr_consent=BOha273Oha273AKASBENCV-AAAAn57_____9_____9uz_Ov_v_f__33e87_9v_l_7_-___u_-3zd4u_1vf99yfm1-7etr3tp_87ues2_Xur__59__3z3_9phPrsk89r6337Ag&c_l=266&c_s=0 |
| https://ps.eyeota.net/pixel?pid=9c9gdbu&sid=26&t=ajs&cat=tv&c_b=1&gdpr=1&gdpr_consent=BOha273Oha273AKASBENCV-AAAAn57_____9_____9uz_Ov_v_f__33e87_9v_l_7_-___u_-3zd4u_1vf99yfm1-7etr3tp_87ues2_Xur__59__3z3_9phPrsk89r6337Ag&c_l=257&c_s=0 |

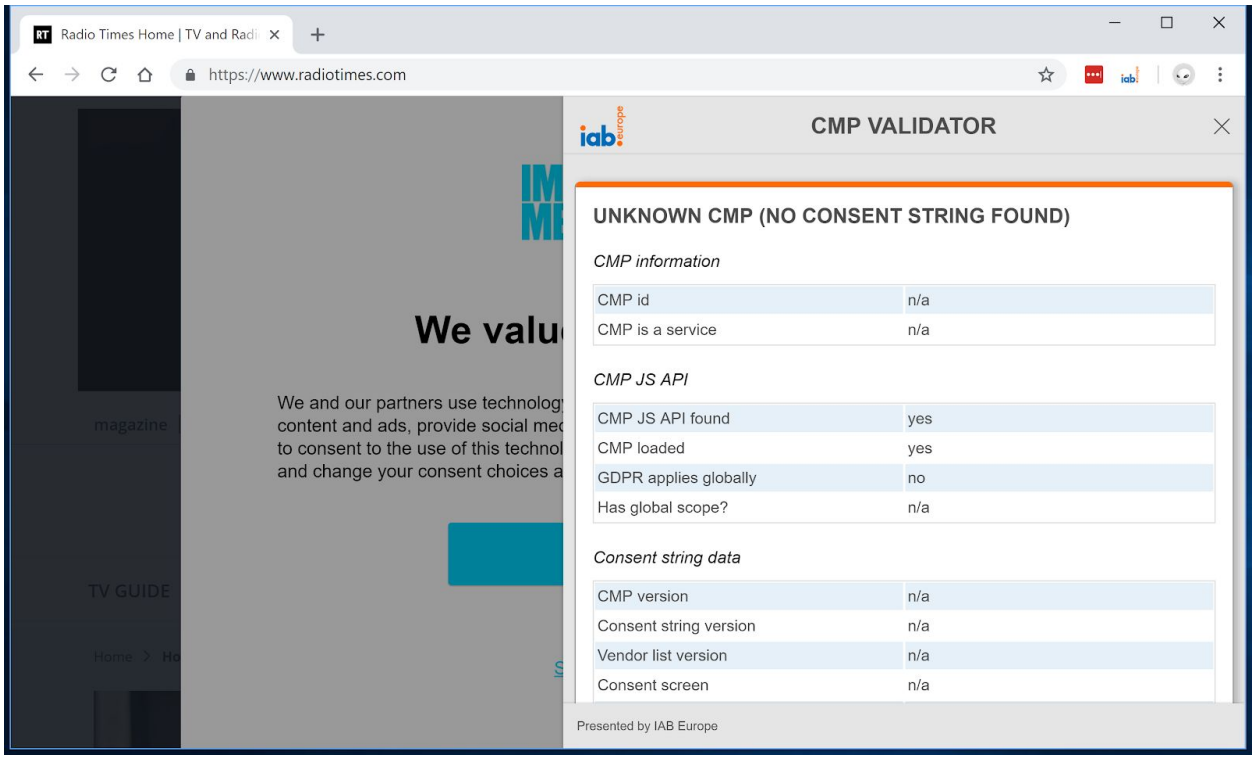
## Summary - tags that contain the consent string

This section shows the number of tags found with the consent string and the maximum length of the URL.

| | |
|---|---|
| Number of tags | 3 |
| Max length (bytes) | 240 |

## No consent string found

If no consent string is found - for example if you run the CMP Validator before consent has been given, you will see the following.




## Information with no value

If a particular data item has no value, it will be shown as ‘n/a’.

# CSV Results

There are three options available in the footer of the Validator that allow to you manage CSV Results.

## Save to CSV

You can save all the results for the current site by clicking on ‘Save to CSV’. The data saved will include the results for all compliance checks as well as all the CMP Information shown. You can save data for multiple sites.

Data saved will persist across browser sessions (browser local storage is used).

***Important note: do not save to CSV from an incognito browser, as the data will not be saved to the same location and will be lost when the incognito browser is closed.***

## Download CSV

Click on ‘Download CSV’ to download all the data for all sites saved to date.

## Clear CSV Results

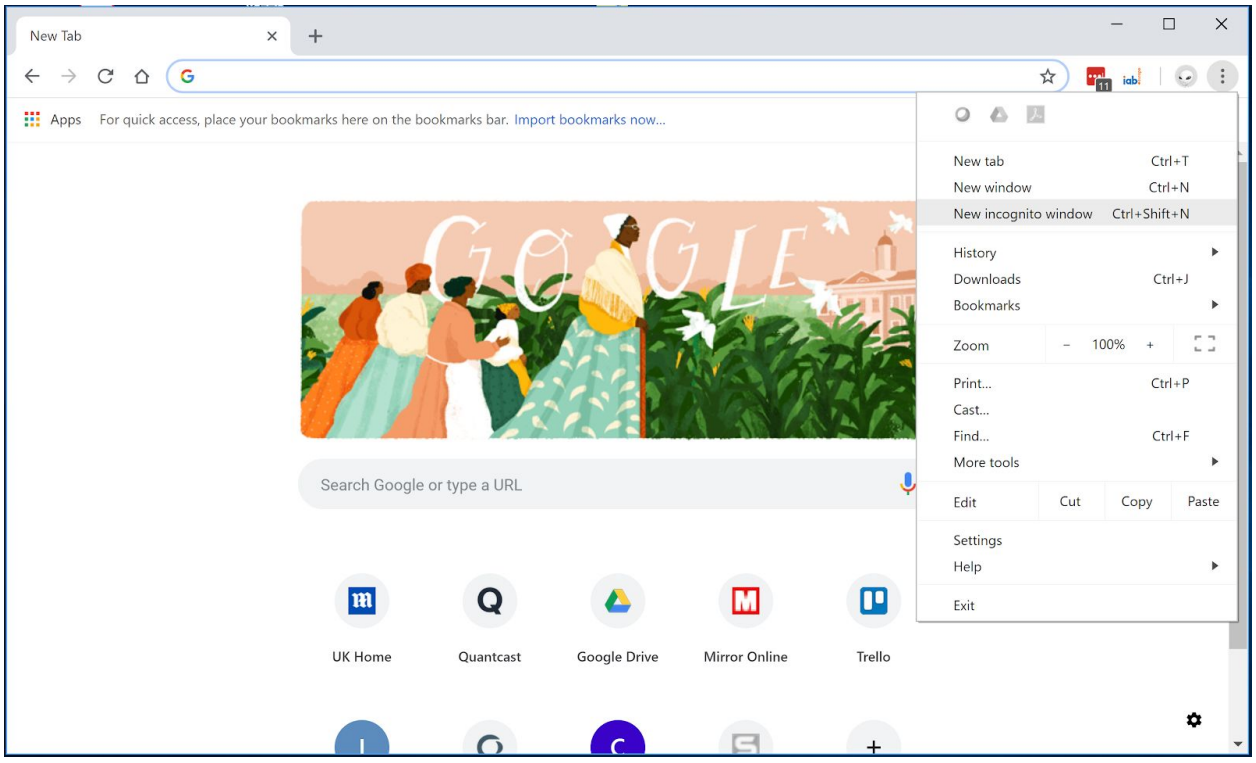
Click on ‘Clear CSV Results’ to delete all CSV data for all sites.

# Testing a site using ‘incognito’ mode

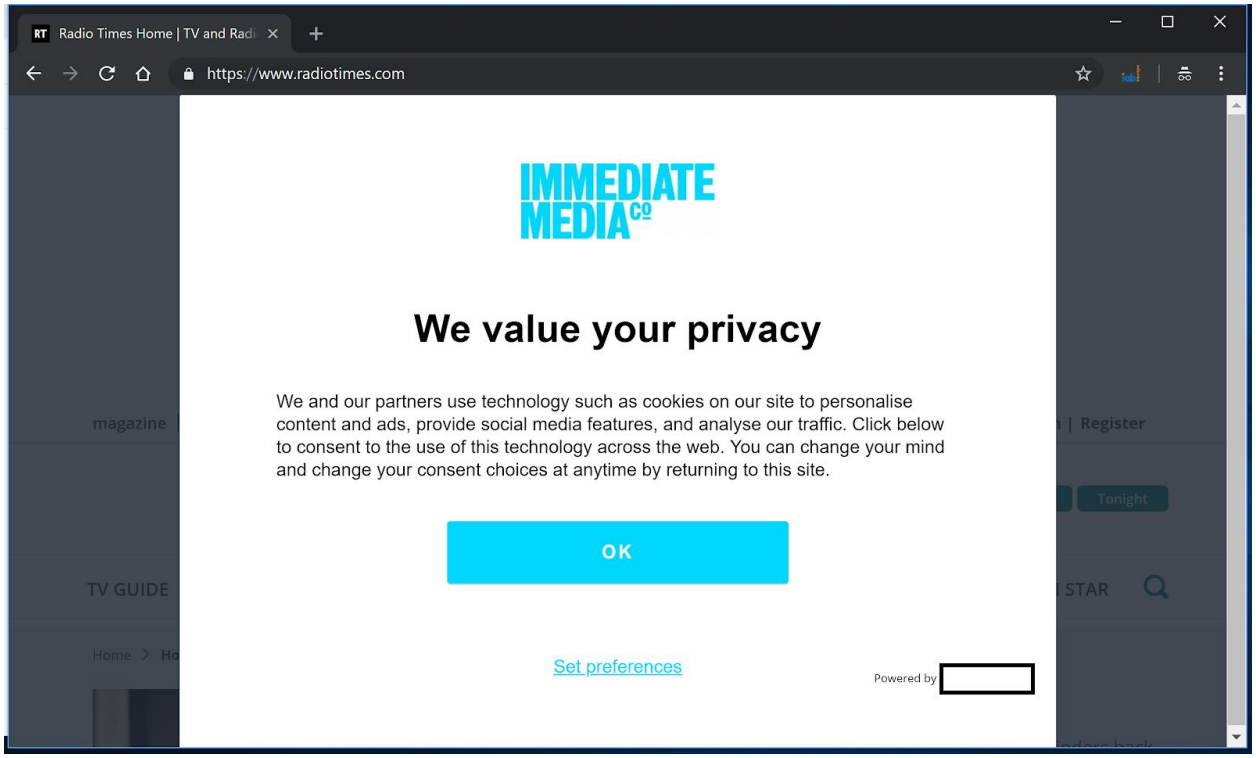
Many of the checks in the Validator require simulating a first time user experience, so that the user interface of the CMP is shown on a given site.

This can be difficult if you have already visited a site, as the CMP will know you are an existing user if a consent string is present and the user interface will not be shown. An easy way to simulate a first time user experience is to launch a window in Chrome’s ‘incognito’ mode. This creates a browser window with a clean slate where there are no cookies and no data in local storage (an alternative browser data storage facility similar to cookies) and therefore allows you to visit a site as a first time user, which should trigger the CMP. Follow these steps to use Chrome’s incognito mode:

1. Choose Settings > New incognito window



2. Visit publisher site - you should see a CMP as a first time user



# I’m a CMP, what do I have to do?

All CMPs must use the Validator to test that their software complies with the technical specifications and policies of the TCF.

This section assumes you have read through this user guide carefully to understand how the Validator works.

As a CMP you must do the following:

1. Run the Validator on a site where your CMP is installed
2. Go through each of the manual checks
3. Send CSV results to IAB Europe
4. Resolve any issues found within 30 days

## Run the Validator on a site where your CMP is installed

Once you have installed the Validator you need to browse to a site where your CMP is running and simulate a first time user experience, so that the consent string analysed by the Validator is created by your CMP and not another CMP (this is only relevant if your CMP is configured for global scope).

If you are a new CMP and have no live installations, you may use a staging site where your CMP is being tested.

Follow these steps:

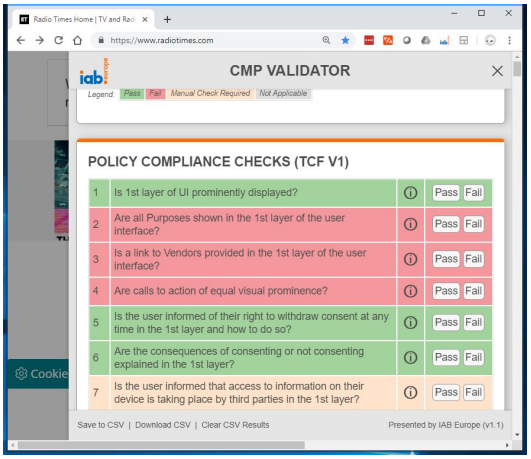
1. Open a standard Chrome browser window (not an incognito window)
2. Browse to a site where your CMP is running
3. Simulate a first time user experience so that your CMP appears - delete any cookies as necessary to trigger your CMP
4. Accept the default settings
5. Run the Validator

The Validator will appear and you will see the results of the technical compliance checks that run automatically. This will be the **main window** where you will register the results of each manual check.

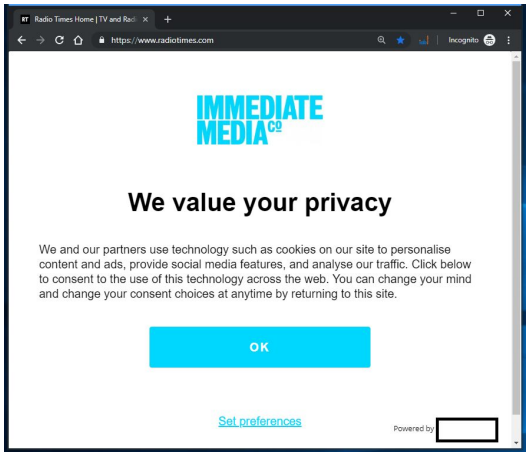
## Go through each of the manual checks

You must now indicate 'Pass' or 'Fail' for each check in the **main window** as stated above. To do this you need to launch a **separate incognito window** for each manual check, determine whether the check has passed or failed, and record the result in the **main window**.

*Main window - record results*




*Separate incognito window for each check*




***Important note: indicating 'Pass' or 'Fail' for a check in an incognito window will be lost when that window is closed. You must ONLY use the main window to indicate the result of each check.***

***Additional important note: if you refresh the page in the main window you will lose all the data entered for manual checks and you will need to start afresh. Opening and closing the Validator will not lose data entered for manual checks.***

Before you run each manual check, click on the info icon (i) which will provide more information about the check and the steps required.

## Send CSV results to IAB Europe

When you have indicated ‘Pass’ or ‘Fail’ for all of the manual checks, you can save your results and send them to IAB Europe.

Follow these steps:

1. Click on the ‘Save to CSV’ option at the bottom of the Validator
2. Download the CSV by clicking on the ‘Download CSV’ option
3. Send the CSV file to tcf.compliance@iabeurope.eu

## Resolve any issues found within 30 days

If any of the checks have failed, you must fix the issues within 30 days and re-send the test results to IAB Europe as above.

Failure to fix all issues will lead to the deactivation of your CMP ID.

# Frequently asked questions

## What is the IAB Europe CMP Validator (the Validator)?

The IAB Europe Consent Management Platform (CMP) Validator is a tool that validates whether a CMP's code conforms to the technical specifications and protocols and policies detailed in the IAB Europe Transparency & Consent Framework (TCF).

## Why was the Validator developed?

Publishers and technical vendors use CMPs to provide transparency, and collect, store, and, where appropriate, share consent information across the advertising ecosystem in order to ensure compliance with the General Data Protection Regulation (GDPR). Today, more than 150 CMPs are registered with the TCF and fall under two categories: (1) those provided for use by multiple publishers and (2) those built in-house by publishers. A CMP's failure to accurately read and record consumers' choices could not only subject publishers and their technical vendors to financial penalties but also reduce publishers' revenue and buyers' opportunities. The IAB Europe CMP Validator exemplifies the association's commitment to support the industry's compliance with GDPR and the longer term commercial sustainability of the industry sector.

## Who developed the Validator?

Developed by IAB Europe, the Validator is a comprehensive testing tool for use by all TCF registered CMPs.  The tool has been developed with ease of usage and comprehensive feedback in mind - it therefore has a UI and a data capture process. It is foremost a tool that has been developed to enable all CMPs to be fully aware of what is needed to comply with the Technical Specifications and Policies of the TCF.

## What was involved in the development of the Validator? Has it been tested in market?

The Validator has undergone a rigorous process of development over a number of months that has involved beta testing and industry feedback throughout. CMP engagement in the process from both categories (service providers and publishers own CMPs)  included Didomi, OneTrust,

Crownpeak, Admiral, Schibsted, Conversant, Quantcast, Xandr as well as Group M and the Guardian. Their feedback has been invaluable enabling IAB Europe to deliver a ‘stand out’ tool.

## Where can I find the CMP Validator and how do I install it? Who can use the Validator?

The Validator is a Chrome extension. This enables the tool to analyse live CMP installations on any site. The tool is only available to CMPs registered with the TCF, or publishers running an IAB TCF registered CMP. To request access CMPs are asked to send an email from their organisation’s domain to: tcf.compliance@iabeurope.eu.

## What operating systems are compatible with the Validator?

The extension can be used in the Windows or macOS versions of Chrome. It is not possible to add an extension to mobile or tablet browsers.

## Does the Validator run on mobile devices?

No, unfortunately browser extensions only run on the desktop version of Chrome. If you have an in-app or non-Web based CMP please submit the appropriate form below as part of the compliance process instead of using the Validator:

- V1.1 non-Web based CMP form
- V2.0 non-Web based CMP form

## I have a non-Web based CMP, can I use the Validator?

No, unfortunately browser extensions only run on the desktop version of Chrome. If you have an in-app or non-Web based CMP please submit the appropriate form below as part of the compliance process instead of using the Validator:

- V1.1 non-Web based CMP form
- V2.0 non-Web based CMP form

## How will the Validator be used in market?

The Validator will be principally used to test new CMPs for compliance before they are published in the registration process. It will also be used to test CMPs prior to annual renewal of their registration. All CMPs who are currently registered in the TCF will be invited by IAB Europe who is the managing organisation (MO) of the Validator to request access to the Validator and complete the test, save and download the results to a CSV file and return this file to the MO. There will be a time limit of 30 working days to return the test on receipt of access to the Validator. All new registrations, post the launch of the Validator, will be required to take the test and demonstrate operational compliance before they are issued with a CMP ID that enables them to participate in the TCF.

## Who verifies the operational compliance of the test?

IAB Europe, the MO of the Validator, will verify the operational compliance of the test.

## What is the validation process for existing CMPs?

All CMPs who are currently registered will be invited to complete the test, save and download the results to a CSV file and return this file to the MO. The MO will confirm if the CMP is successfully validated.

## What is the validation process for new CMPs?

All new CMP registrations will be required to take the test and demonstrate operational compliance before they are issued with a CMP ID that enables them to participate in the TCF.

## Will all Validator testing be managed by CMPs on a self-assignment basis?

All CMPs will be asked to take the test and return their results to the MO. The MO will also run monthly independent checks on CMP installations on publisher sites and follow up any failed tests.

## If a CMP does not pass the validation tool operational requirements, what will be the next steps?

If a CMP returns a test that shows failures then the MO organisation will ask the CMP to rectify the failures within 30 days, re-run the test and return their results.

## Who will be informed if a CMP does not comply in the given timeframe?

In the instances where a CMP has failed a test and does not rectify the failures within the given period of 30 days the CMP will be advised by the MO that they have 14 days to complete a successful test after which their CMP ID will be deactivated. The community of registered TCF Vendors will be advised that the CMP ID that has failed the test is deactivated until further notice. The CMP will be asked to notify ALL publisher sites that are using their CMP.

## Will the MO make public the results of the testing?

The MO will notify all vendors as part of the operational management of the TCF that a Consent String sent by a CMP deactivated from the Framework is no longer valid. The CMP will also be removed from the list of registered CMPs. The Validator is principally a tool to support those who are operating in the Framework. Test failures can arise for a variety of reasons and in most instances we anticipate that any issues that the test identifies will be resolved swiftly. The test is there to support the community of CMPs and ensure that they fully understand both the technical specification and the Policy of the TCF. Ultimately providing, in the first instance, a guide for the MO and the CMP. Therefore only test failures that result in deactivation will be more widely notified.

## What does the MO hope to achieve through the implementation of the Validator?

There are 180 plus companies registered as CMPs in the TCF. Each of these organisations must build functionality from the common technical specification that will interact flawlessly with other organisations in the digital advertising ecosystem. It is incumbent upon the industry to ensure that the organisations listed as CMPs are in fact able to perform in that role and that the success of the TCF is not undermined by ‘actors’ who do not correctly interpret the TCF

protocols. The MO is therefore committed to working with the registered CMPs to ensure that all are compliant in the context of the Validator.

## Is it likely that the Validator will accelerate CMP deactivations? What will be the impact on the TCF?

The Validator has been developed to support CMPs with the implementation of the TCF and the compliance of publishers' websites with GDPR. It is hoped that all registered CMPs will respect this important investment made by the MO and will work collaboratively as a community to ensure that operational compliance is achieved by all. This respect must go 'hand-in-hand' with the understanding that compliance is crucial to the success of the TCF and that the MO needs to have the facility to enforce. It is not anticipated that this will result in a level of deactivation that will negatively impact the TCF but will drive higher levels of exemplary implementations.

## Is the Validator able to test for both TCF version 1 and TCF version 2 operational compliance?

The Validator in its first iteration has been built to test TCF version 1 compliance. There will be in due course an iteration of the Validator that will test TCF version 2 operational compliance.

## If a complaint is raised with a DPA about a CMP registered with the TCF, what is the process?

On receiving notification of a complaint from a DPA the CMP will be deactivated from the Framework by the MO. An investigation into the cause for complaint will then be led by the MO, liaising with both the CMP and the DPA as appropriate.

## What is the deactivation process?

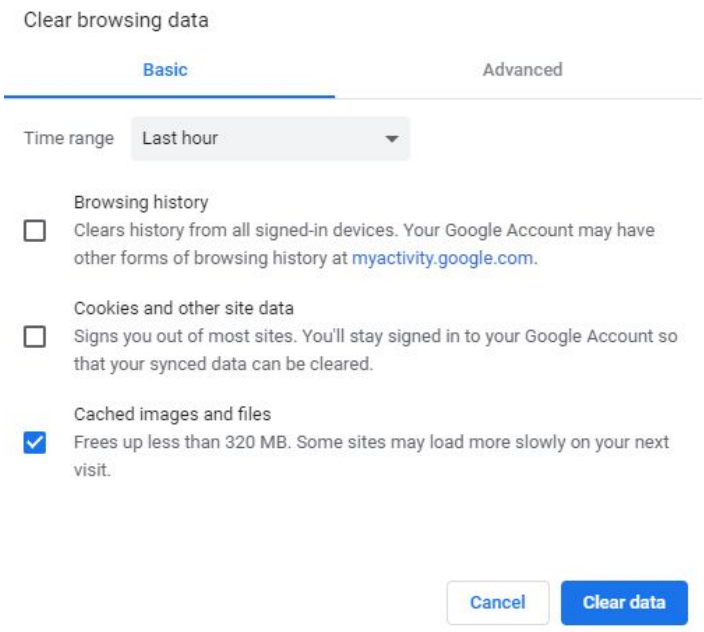
CMPs that register with the TCF are issued with a CMP ID number and a DNS zone for their consensu.org sub-domain. If a CMP is deactivated their ID is removed from the CMP registration and their DNS zone is deactivated. Additionally all vendors who are registered in the TCF are advised that the CMP ID is deactivated and any consent strings generated by this CMP ID are invalid.

## What is the enforcement process?

The enforcement process starts after a failure of a Validator test. The CMP is advised they have 30 days to implement development changes to ensure a successful test. Post the 30 day period that closes with a continuing failure of the test the CMP is advised that their CMP ID will be deactivated within 14 days. The exception to this process is a deactivation that results from a DPA notification. In these instances CMP ID deactivation is immediate.

## How do I get the latest version of the Validator?

The Validator is self-updating. Most of the time you will simply be using the latest version of the Validator without realising it. If there has been a recent update and you cannot see a new feature, you may need to clear your cache:

**Settings > More tools > Clear browsing data…**

Make sure you only clear ‘Cached images and files’ for the last hour to avoid logging yourself out of other sites.