CSI-COP

Citizen Scientists Investigating Cookies & App GDPR Compliance

Coventry University, UK
Stelar, Germany,
Immer Besser, Germany,
Universitat Autonoma de Barcelona, Spain
Bar Ilan University, Israel
Czech Technical University Prague, Czech Republic
University of Oulu, Finland
Association of Hungarian Women in Science, Hungary
University of Patras, Greece
Acknowledgements: CSI-COP Citizen Scientists, CSI-COP stakeholders, and Xcel Resources Ltd.

September 2023

Guidelines to Implement Privacy-by-design in EU-funded project Communication Tools Complying with the GDPR.

These Guidelines are part of a project that has received funding from the **European Union's Horizon 2020 research and innovation programme under grant agreement N°873169**

Table of Contents

These Guidelines are part of a project that has received funding from the
European Union's Horizon 2020 research and innovation programme under grant agreement N°873169

Guidelines

These Guidelines are as a result of the scientific work of CSI-COP consortium partners CSI-COP's citizen scientists, innovation sub-contractor, and stakeholder engagement during the project. These Guidelines emerged from CSI-COP (GA 873169), a *Horizon2020 science with and for society* (SwafS) 15-2018/2019 call for 'exploring and supporting citizen science'. The Guidelines are intended to provide a road map enabling the European Commission to improve compliance of the general data protection regulation (GDPR – EU 2016/679).

The Guidelines contain a **roadmap** of five simple steps to make it simpler for the European Commission to monitor GDPR compliance specifically in websites and apps. The Guidelines recommend that the European Commission begins with step 1: reviewing its own suite of websites and advocated apps with respect to transparency of text in cookie notices and privacy policies.

Further policy-making discussions might include methods to make it easier for citizens in the EU to contact their country's data protection authority, to report websites and apps that contain dark patterns or contain opaque statements from third-parties around 'legitimate interest' for extracting personal data. Additionally, a web or app 'trust badge' or 'traffic-light system' could reward GDPR-compliant transparent websites and apps that provide clear information on purpose and seek informed consent for requesting personal data from visitors and users.

Additionally, the Appendix offers Best Practice Guide for website and app development. The Guidelines for the European Commission and the Best Practice Guide provide realistic information to improve implementation of the GDPR and monitor compliance of personal data protection in EU funded projects.

Contact for further information:

Dr. Huma Shah, CSI-COP Coordinating Partner, Coventry University- email: ab7778@coventry.ac.uk

These Guidelines are part of a project that has received funding from the
European Union's Horizon 2020 research and innovation programme under grant agreement N°873169

CSI-COP ROADMAP for the European Commission

1. Step 1: the European Commission reviews its own suite of web pages across its Internet platforms and any apps it advocates (Figure 1).

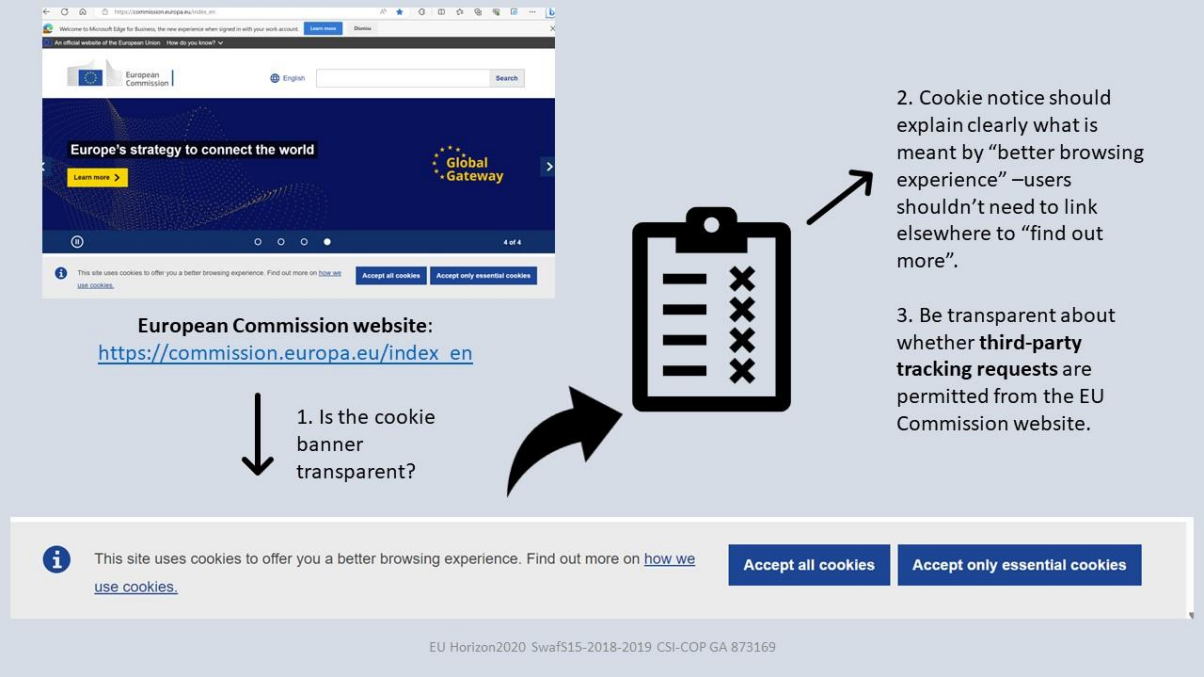


Figure 1: Step 1: Review Cookie banner on European Commission website.

Building trust with website visitors and app users would benefit from a clear and visible cookie banner or cookie notice, at the top or bottom of a website or in the app information. This also accords with the **EU's Digital Services Act** (DSA, 2022): better services and new rights for consumers, and more transparency. Figure 1 above shows the European Commission website main page featuring a cookie banner at the bottom of the screen.

Step 1 should involve:

a) Reviewing the cookie banner on European Commission pages: could it be made clearer for the website visitor precisely what "all cookies" and "better browsing experience" refers to? Should the user be expected to select a link to learn more about *how cookies are used*?
b) Would a **simple-to-understand label** 'Privacy Policy' and link to it be better?
c) Can a Privacy Policy be crafted so that non-legal and non-technical visitors could understand unambiguously whether personal data is being collected through cookies and whether that data is shared with third-parties?

An example of a clear cookie notice is taken from the CSI-COP project website:

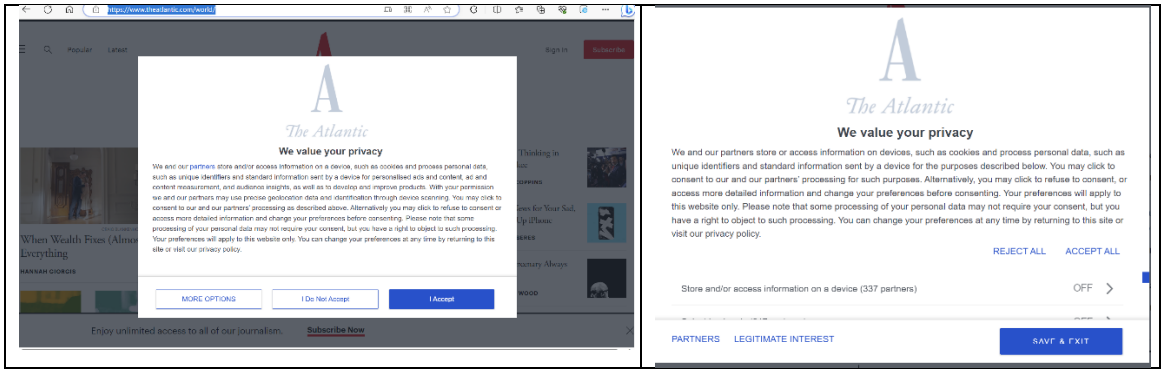
Screenshot 1: CSI-COP cookie banner: https://csi-cop.eu/

These Guidelines are part of a project that has received funding from the
European Union's Horizon 2020 research and innovation programme under grant agreement N°873169

CSI-COP website cookie banner at the bottom of its home clearly conveys that it does not track its visitors.

2. Step 2: The European Commission reviews its legal definition for '**Legitimate Interest**'.

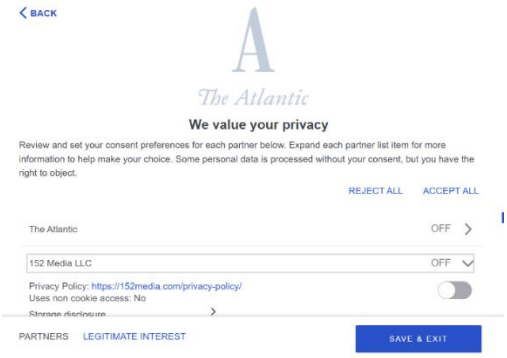
Legitimate interest appears to be an excuse to extract personal data without clear reasons why and what the benefit is to the consumer. Examples of the numerous 'Legitimate Interest' vendors is provided here from just one website for "news, literature and opinion" – The Atlantic. This magazine has featured seminal articles, such as 20thC American engineer and inventor **Vannevar Bush**'s 'As We May Think', a 1945 visionary missive presenting ideas on an information society with thinking machines. **The Atlantic**'s online magazine is accessible by European citizens in Europe. The website contains numerous vendors named with 'Legitimate Interest' to extract information from its visitors. Investigating on 25 August 2023, the Atlantic magazine presented a cookie wall between its featured articles and its visitors (Screenshot 2: left). The cookie wall provides information on its privacy practice including the statement: "we and our partners store and access information on a device" (Screenshot 2). The cookie wall offers three options: including 'More Options.' Selecting 'More Options' leads to further options: 'Partners' and 'Legitimate Interest' (Screenshot 2: right).



Screenshot 2: (Left) The Atlantic Magazine cookie wall; (right) Partners & Legitimate Interest
https://www.theatlantic.com/world/

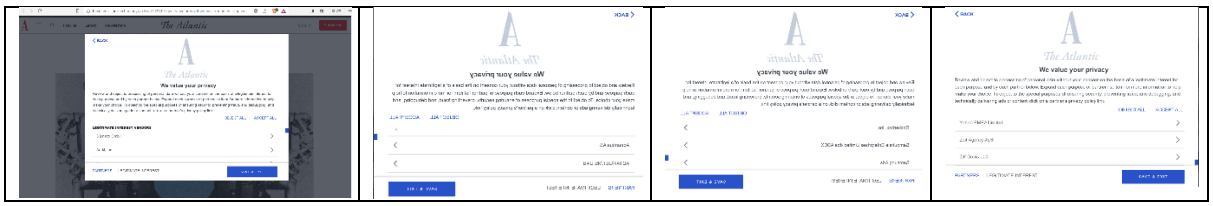
Selecting 'Partners' brings up a list of organisations with links to find out more about these third-parties' Privacy Policies starting with '152 Media LLC', an AdTech company concerned with monetising website revenue. Two options are offered in 'Partners' including 'REJECT ALL' (Screenshot3).

These Guidelines are part of a project that has received funding from the
European Union's Horizon 2020 research and innovation programme under grant agreement N°873169



Screenshot 3: The Atlantic magazine's 'Partners'

Checking The Atlantic magazine's 'Legitimate Interest' presents another series of third-party organisations: 'Legitimate Interest' vendors ((Screenshot 4). The 'Legitimate Interest' vendors list start with 3Q nexx GmbH – apparently concerned with online streaming. Two options are offered in The Atlantic magazine's 'Legitimate Interest' cookie wall, including OBJECT ALL (Screenshot 4).



Screenshot 4: The Atlantic magazine's 'Legitimate Interest': https://www.theatlantic.com/world/

The list of vendors with 'Legitimate Interest' beneath 'The Atlantic' online magazine website appears endless as you scroll down to find out *who they are*, and precisely what their *legitimate interest is* to access 'The Atlantic' online magazine's visitors. Legitimate Interest is an opaque term with no clear information on any benefit to the website visitor. The benefit is to the 'Legitimate Interest' vendor who, as a third-party (see CSI-COP Taxonomy, 2023) can perform unwanted measurements of ads, provide 'personalisation' and "Apply market research to generate audience insights" (beneath cookie wall in 'Legitimate Interest' in The Atlantic- August 2023).

It is clear that businesses need customer data to thrive in highly competitive markets. However, the Internet has become a confusing place for users who cannot know for sure if they have truly rejected unwanted tracking through 'partners' and objected to 'legitimate interest' requests from unknown vendors, including the advertising technology industry. The 'Legitimate Interest' pretext does not appear to comply with the GDPR's principles of transparency, informed consent, and purpose limitation. With new Internet innovations, such as evolved 'search' in Internet browsers incorporating large language models - LLMs (e.g., Microsoft's Bing using ChatGPT; Google's Bard) powered by Artificial Intelligence (**AI**), it is imperative that the definition of 'Legitimate Interest' fits in with the EU's strategy for AI to better preserve consumers personal data online. Hence CSI-COP project recommends that the EU review its definition of 'Legitimate Interest' to help people better understand whether their personal data is being harvested without full informed consent.

These Guidelines are part of a project that has received funding from the
European Union's Horizon 2020 research and innovation programme under grant agreement N°873169

3. Step 3: The European Commission implement a separate and specific GDPR-transparency and purpose limitation question in future EU grant programmes in EU proposal submission stage.

In the EU grant proposal preparation stage consortia must complete a series of questions from 'scope of application' as part of their grant bids. CSI-COP recommend that an additional and specific question be added for website and app GDPR compliance. For example, questions for EU project proposers include:

- **Use of human embryonic stem cells (hESC): YES/NO**
- **Do no significant harm principle: YES/NO**
- **Exclusive focus on civil applications: YES/NO**
- **Artificial Intelligence: YES/NO**

CSI-COP Guidelines recommend that in future EU grant programmes add an additional question specifically about data protection and online privacy in project websites and apps, such as

- GDPR compliance in project websites and apps: Do the communication activities proposed follow a privacy-by-design approach to protect personal data of citizens, so comply with the principles of transparency and informed consent and purpose limitation in project websites and apps?

Such a question would involve making EU grant proposers consider the purpose of including any third-party tracking tools in project created websites and apps, and the need to make this transparent.

4. Step 4: The European Commission offers Technical Guidance realised from the CSI-COP project for EU funded project privacy-by-design websites and apps

It is possible to construct privacy-by-design websites and apps deploying available web and app development platforms. EU Horizon2020 SwafS15-2019 funded CSI-COP project (2020-2023: GA 873169) deployed **WordPress** while prioritising a privacy-by-design philosophy. CSI-COP's cookie notice made it clear that visitors were not tracked across the project's web pages (see Screenshot 1). Embedded third-party tracking cookies in WordPress web development environment were extracted for CSI-COP's website. CSI-COP's Privacy Policy was crafted to make it simple to understand that no analysis of visitor traffic was enabled. It does not require knowledge around legal technology to understand CSI-COP website's cookie notice and Privacy Policy, and that the project does not permit third-party tracking.

WordPress offers numerous plugins for uploading and making publications available either online or for download. Additionally, there are plugins available for maintaining count of visitor views or downloads. However, it is important to note that if any of these plugins make third-party requests outside of WordPress, those should be blocked

These Guidelines are part of a project that has received funding from the
European Union's Horizon 2020 research and innovation programme under grant agreement N°873169

using custom scripts or security header policies. Further technical information on this can be requested from CSI-COP sub-contractor, Xcel Resources Ltd., and their privacy-by-design software engineer, Mr Venkatesh Nanneboina, email: venkatesh@xceltech.co.uk

EU grant recipients can similarly ensure they specify privacy-by-design as a key requirement to prospective web development teams. Web developers entrusted with creating EU funded project websites should ensure they adopt privacy-by-design.

Additionally, app design for project interaction with citizens and data collection can follow privacy-by-design. App developers can be required to extract third-party tracking code in the development environment, and set app permissions for only those functions that are necessary for the app to work. EU funded project apps should not require access to people's contacts, messages, photos, camera, and microphone unless the purpose is made clear and explicit. App design should also follow transparency, informed consent, and purpose limitation principles of the GDPR.

5. Step 5: The European Commission Standardises Cookie Notices and Privacy Policies

The European Commission could advocate standard text for cookie notices and privacy policies to make it easier for its funded projects to comply with the GDPR. CSI-COP investigated over 100 EU funded projects for its web-based, open-access knowledge resource of digital tracking: CSI-COP Repository. Not all EU funded projects investigated in CSI-COP were shown to fully follow GDPR principles. This conveys some disconnect between Project Management and Partners entrusted with project web development. CSI-COP have been awarded standardisation support through the EU's HS.booster initiative. CSI-COP will be working towards producing a standard that could be used in website and app cookie notices and privacy policies to make it clearer to users how their personal data is treated. This CSI-COP legacy intends to contribute to improving societal trust between citizens and scientists, increasing scientific literacy, and expanding privacy-by-design to reverse the surveillance economy that now pervades the Internet.

Summary

These Guidelines emerge from the scientific work of CSI-COP partners, CSI-COP citizen scientists, CSI-COP Repository innovation sub-contractor, and stakeholder engagement. The five simple steps presented in these Guidelines are designed to equip the European Commission with timely information from the research and innovation realised in the Horizon2020 SwafS15-2019 funded CSI-COP project (GA 873169). Implementing CSI-COP's Guidelines could improve compliance of the GDPR in project websites and apps in the projects that the EU funds. In this way the European

These Guidelines are part of a project that has received funding from the
European Union's Horizon 2020 research and innovation programme under grant agreement N°873169

Commission would be leading the way to transform the Internet back to a place for knowledge-sharing and invaluable connections.

These Guidelines are part of a project that has received funding from the
European Union's Horizon 2020 research and innovation programme under grant agreement N°873169

Appendix

Best Practice Guide for Website and App Development

Introduction

CSI-COP's Best Practice provides guidance on how to design a GDPR compliant website or App applying a privacy-by-design approach. Unfortunately, many website and App Development tools automatically build in tracking technologies of one sort or another. As part of the EU funded CSI-COP project the decision was taken to build its project website to ensure that minimum or preferably no cookies or tracking technologies (https://csi-cop.eu/) were incorporated. This WordPress website can be used by any EU funded project as a baseline for their own project website. Please note that if you add any plugins or components that were not part of the original CSI-COP website design then trackers may be incorporated. The website is dynamic and will therefore adjust automatically to mobile phones and/or tablet devices. This is the simplest way to construct an App which incorporates Privacy By Design. App development tools normally require significant technical knowledge to remove in-built tracking technologies.

The appendix covers:

- Best Practice in Cookie and Tracker Consent
- Best Practice in Cookie and Tracker Customisation Options
- Deciding whether a site needs cookies and tracking technologies
- Using Cookie Consent and Management Systems or manage your own site
- Checking a Website for Cookies and other Tracking Technologies
- Creating a Privacy Notice
- Considering Web Accessibility

Best Practice in Cookie and Tracker Consent

The first thing any visitor should see when they visit your site is a Cookie or Tracker Consent banner. Good practice should include:

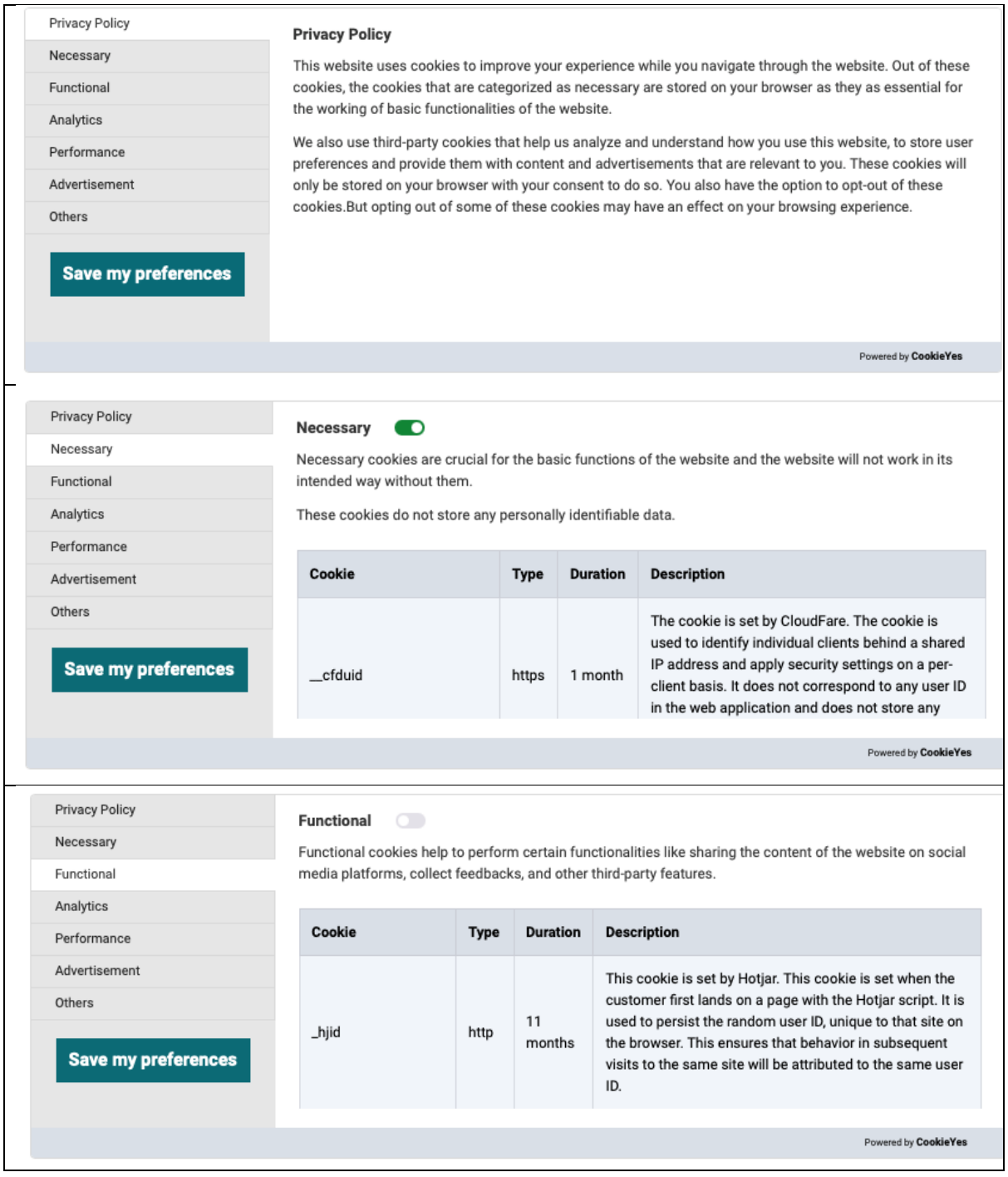
- The banner is visible, readable and uses clear non-legal language
- The reason for using cookies is clearly explained
- The options to manage cookie preferences are equally prominent
- There is a clear link to the Cookie Notice
- The Cookie Banner remains visible until the user makes a selection

Best Practice in Cookie and Tracker Customisation Options

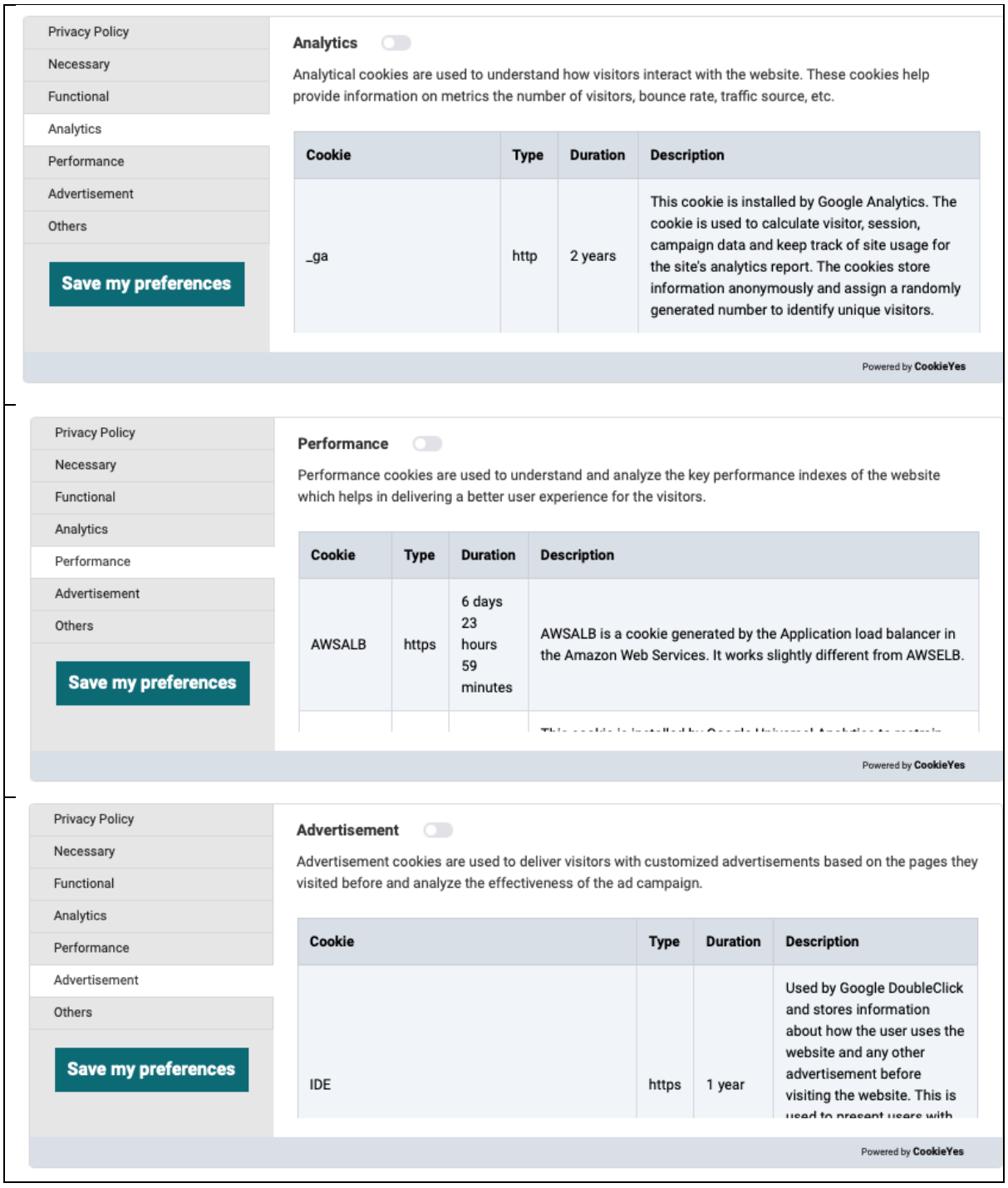
Options should be made available for website visitors to make informed choices. Option such as "Manage My Choice" or "Customise My Settings" should be offered clearly layout the necessary cookies. It should be made clear if there are tracker technologies and why. **The default option should be no third-party tracking**. The other options should clearly group using a sensible categorising that defines the

These Guidelines are part of a project that has received funding from the
European Union's Horizon 2020 research and innovation programme under grant agreement N°873169

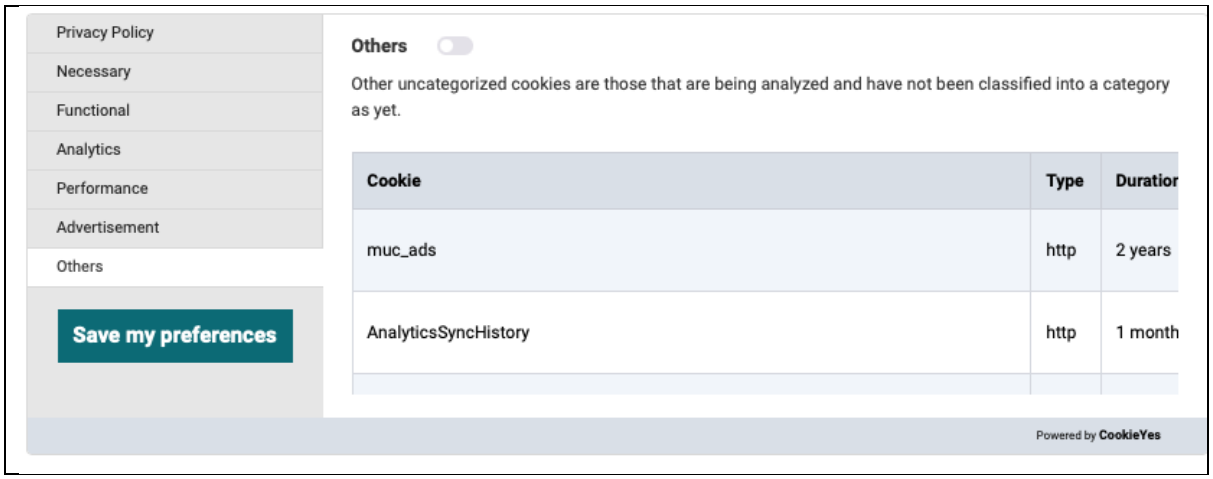
function of the cookies and tracking technologies used on the website. See example from the Coventry University Website below:



These Guidelines are part of a project that has received funding from the
European Union's Horizon 2020 research and innovation programme under grant agreement N°873169



These Guidelines are part of a project that has received funding from the
European Union's Horizon 2020 research and innovation programme under grant agreement N°873169



https://www.coventry.ac.uk © CookieYes 2023

For each category used there should be:

- A simple option to positively select or exclude this category
- A brief description of the category and what it does if selected
- A list of cookies in this category with type, duration, and a brief description of the function of the cookies or tracker technology used on this website

It is best practice to provide 5 to 7 clear options website visitors can read, understand decide and select quickly. Convenience of 'Accept All' should be avoided because this type of option does not make it clear what 'All' means precisely.

One of the main reasons for web managers to use cookies is to be able find out more about their users and their interaction with the website. Normally this involves using a third-party tool, but this might not be compliant with the GDPR depending on if the information it provides also finds itself outside of the European area. There are an increasing number of privacy-focussed analytic tools which provide cookie-less access to website and user date.

- https://wordpress.org/plugins/burst-statistics/
- https://matomo.org/
- https://usefathom.com/ref/ZGTPES
- https://plausible.io/
- https://www.simpleanalytics.com/
- https://getinsights.io/

Using Cookie Consent and Management Systems or manage your own site?

It is possible for small or static websites to manually manage cookie banners, detection, and management. However, most large, and dynamic websites these days make use of a third-party Cookie Consent and Management system such as CookieYes (https://www.cookieyes.com/). This and below are not specific

These Guidelines are part of a project that has received funding from the
European Union's Horizon 2020 research and innovation programme under grant agreement N°873169

endorsements as there are a large number of these service providers offering different levels of support at different prices:

- https://cookiefirst.com/
- https://usercentrics.com/
- https://www.onetrust.com/products/cookie-consent/
- https://www.osano.com/

Cookie Consent and Management system typically provide:

- Cookie banners in multiple languages
- Cookie control to allow user choice of cookies
- Cookie scanning to auto detect and categorise cookies
- Consent management to record user's choices
- Policy generators to provide policies for websites
- Non-technical integration into websites built using a wide range of Content Management System (CMS)

Some of these systems provide a free service for a small website, or charges monthly subscription for large websites.

Checking the Website for Third-party Cookies and other Tracking Technologies

As you are building your project website it is essential to regularly check that you have not introduced third-party cookies or tracking technologies unless you want them. They should not be included as default, a clear option to reject should be provided. This could happen by introducing a plugin or third-party module. It is good practice to scan the website with a cookie tracker, then make a backup copy of your website, before adding the new plugin or module. Following which, scan the website to see what cookies or tracking technologies have been added. If the added cookies cannot be easily disabled or removed, you can revert to the backup copy.

There are range of easy-to-use cookie and tracking technology detection tools for websites:

- https://themarkup.org/blacklight
- https://webbkoll.dataskydd.net
- https://www.cookieserve.com/
- https://termly.io/products/cookie-scanner/
- https://sitechecker.pro/cookie-checker/
- https://www.cookiemetrix.com/
- https://www.cookieyes.com/cookie-checker/?ref=SB_24022022c
- https://www.cookiemetrix.com/

Creating a Privacy Notice

As part of the GDPR every website must have an accessible privacy notice which should be written in terms that are easily understandable and not cloaked in legal

These Guidelines are part of a project that has received funding from the
European Union's Horizon 2020 research and innovation programme under grant agreement N°873169

terms. The EU already provide clear guidance and a template to help projects develop their own privacy notice. See https://gdpr.eu/privacy-notice/

Considering Web Accessibility

Whilst not directly part of the CIS-COP project it is worthwhile considering website accessibility as part of the overall design. All official websites of EU institutions should follow international guidelines for accessible web content. This means that texts, images, forms, sounds, etc. should be accessible and understandable by as many people as possible without discrimination. WC3 Web Content Accessibility Guidelines (WCAG) 2 Level AA Conformance provides a target level of accessibility (https://www.w3.org/TR/WCAG22/). The EU Europe site provides detail support and guidelines on accessibility requirements https://wikis.ec.europa.eu/display/WEBGUIDE/12.+Accessibility.

The achievement of the standard involves using checklists to consider the various element of website design that can only be addressed by human observers. However, the WAVE Web Accessibility Evaluation Tool provides an automated overview of issues that potentially affect accessibility https://wave.webaim.org/). a similar tool is available for testing accessibility on mobile websites (https://ready.mobi/).

Conclusion

This is Best Practice Guide looks at how to design a GDPR compliant website or App to support EU funded projects that minimises cookies and trackers. It covers:

- Best Practice in Third-party Cookie and Tracker Consent
- Best Practice in Third-party Cookie and Tracker Customisation Option
- Deciding if the site needs cookies and tracking technologies?
- Using Cookie Consent and Management Systems or manage you own site?
- Checking the Website for Cookies and other Tracking Technologies
- Creating a Privacy Notice
- Considering Web Accessibility

As part of the EU funded CSI-COP project website was designed that had no cookies or tracking technologies (https://csi-cop.eu/) incorporated. This WordPress website can be used by any EU funded project as a baseline for their own project website. Please note that if you add any plugins or components that were not part of the original CIS-COP website design then trackers may be incorporated.

These Guidelines are part of a project that has received funding from the
European Union's Horizon 2020 research and innovation programme under grant agreement N°873169