

Cyberwomen Data Use Policy

contacto@cyber-women.com

**INSTITUTE FOR
WAR & PEACE REPORTING**



© 2019– Institute For War And Peace Reporting

<https://iwpr.net/>



This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) license.

<https://creativecommons.org/licenses/by-sa/4.0/deed.en>

Contents

1 Cyberwomen Data Use Policy	5
Context	5
About the project	5
The Right to Privacy	6
Regulations	6
Compliance	7
Cyberwomen's commitment to privacy	7
What we are doing	8
Cookies and third party code	8
Communications	8
Logs and web statistics	9
Javascript	9
Changes to this Policy	10
Contacts	10
What you can do	10
How do I change my cookie settings?	11

Chapter 1

Cyberwomen Data Use Policy

This document was last updated the 4th of September of 2018. Written by Kéfir.

Context

Before plunging into specific details on how we use the data generated on this site and what you can do to be more agent in all of this, we are going to give some context.

About the project

The Cyberwomen curricula was created and implemented by the Institute for War and Peace Reporting as part of the project Safety, Awareness and Action (SAWA) and funded through the Bureau of Democracy, Human Rights and Labor (DRL) at the U.S. Department of State.

The web platform was designed and developed by Kéfir¹, as well as the frontend web and graphic design. Kéfir, until present, administers the server where this project is hosted.

You can read more about the Cyber-Women project here².

The Right to Privacy

The Right to Privacy is defined as a human right, explicitly stated under Article 12 of the 1948 Universal Declaration of Human Rights:

“No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.”

Regulations

Apart from human rights, there are specific data regulations. Perhaps you have heard the recent GDPR?

The “General Data Protection Regulation”³ came into effect the 25th of May of 2018.

This European regulation is designed to better protect citizens from data breaches and privacy violations. The new law is amongst other things stipulating how companies must handle their customers' data.

Unfortunately, these regulations aren't applicable in all contexts and they are not enough standing alone. Certain jurisdictions have a fairly good understanding and coverage of privacy; others are far behind. There are groups and people that, from the policy front-lines, are fighting to change this unequal access to privacy.

¹<https://kefir.red/>

²<https://cyber-women.com/en/#about>

³https://en.wikipedia.org/wiki/General_Data_Protection_Regulation

Have a look at the Association for Progressive Communications network's statement on GPDR⁴.

Compliance

All websites and platforms visited by citizens that are protected by data regulations must provide a compulsory legal document that explains how they collect, retain and share personally identifiable information.

Personal Identifiable Information (PII) is any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly. Examples of sensitive PII elements include, but are not limited to: name, social security number, driver's license and other government identification numbers; citizenship, legal status, gender, race/ethnicity; birth date, place of birth; home and personal cell telephone numbers; personal email address, mailing and home address; religious preference; financial information, medical information, disability information; spouse information, marital status, child information, emergency contact information.

Collecting and using data doesn't necessarily have to be a harmful. Data is used for satisfying legal and funding-related reporting requirements and improving tools. What is important is that there is transparency of how data will be collected, stored, processed and shared.

Cyberwomen's commitment to privacy

Beyond complying certain minimums, this platform, in it's bones and code, was designed and developed by activists to pursue and embed privacy as a value and ethical standpoint and practice.

We don't just avoid identifying individuals but believe in not generating data that can be used for interests that aren't aligned with those of whom visit this platform.

⁴<https://www.apc.org/fr/node/34716>

Typically, data use policies are abstract, lost in small print and quite cryptic. This reflects a lack of transparency and accountability, normally with the intention of hiding the details of a data business model and collaborations with third parties that users wouldn't be happy to find out about.

In Cyberwomen, our Data Use Policy is an extension of the project: an opportunity to learn about our right to privacy, how it can be taken into account and what specific measures we can apply.

What we are doing

Cookies and third party code

When you visit a webpage parts of the page may come from domains and servers other than the one you asked to visit. This is an essential feature of hypertext, but it has also come to be a serious privacy problem. On the modern Web, embedded images and code often use cookies and other methods to track your browsing habits – often to display advertisements. The domains that do this are called “third party trackers”

Internet cookies are, ultimately, text files that a website stores in your computer when you visit so that, in potential future visits, it “remembers” information like your language preference or your log-in.

The CyberWomen platform doesn't use cookies or any type of third party code.

Communications

Websites that include contact forms must describe why they are asking for such information and what they are going to do with it afterwards. For example, if it going to be used for a newsletter or a database.

Cyberwomen doesn't use contact forms. It does have associated email accounts so people can contact with the project (contacto@cyber-women.com)

and request information related with privacy aspects (privacy@cyberwomen.com).

These mail accounts are also administered by Kéfir that commit to implementing up-to-date security measures, maintaining non-identifiable data logs that are collect only information strictly necessary for it's functioning and that are deleted after one week.

The email accounts are accessed via webmail and email clients, taking into account security practices mentioned in the curricula.

Logs and web statistics

A log is a record. Services and applications that run on a device tend to save some type of record. This provides information when improving tools and solving possible errors. Generally this information is useful but it contains personal identifiable information like IP addresses and usernames that can be used to create fairly accurate profiles about people's behavior. This is why it is important to anonymize logs in a secure way.

Kéfir's servers don't log any IP addresses, just anonymized visits, which we remove after a week.

Cyberwomen collect statistics, through <https://sinapsis.kefir.red>, Kéfir's self-hosted version of Piwik/Matomo⁵, which means only IWPR and Kéfir have access to this data. It is configured to not log any information that may identify individual visitors, like IP addresses. Also, all individual visits are converted into statistic data and then discarded after a month. Matomo also respects the Do-Not-Track feature browsers specify as a way to opt-out of these kind of systems.

Javascript

The Cyberwomen site uses javascript.

⁵<https://matomo.org/>

- zepto.min.js: Zepto⁶ is a minimalist JavaScript library for modern browsers with a largely jQuery-compatible API
- agency.js: Cyberwomen is based on Agency Jekyll Theme⁷. This javascript gives the site a responsive menu behavior.

If you disable javascript (using Tor Browser Bundle, through a plugin or through your browser configuration), the site will continue to work. On small screen devices, the menu will appear at the bottom of the page.

Changes to this Policy

This document may be updated in the future. Come back to this page to see updates.

Contacts

All questions related to the Data Use Policy can be sent to privacy@cyber-women.com.

What you can do

You can also contribute to your privacy. The fact that on our side we don't collect data that you don't consent to, that we store it for a limited time in a anonymized way and don't share it with third parties beyond general information for funding report back purposes doesn't mean that other potential intermediaries are vulnerating your privacy.

- Read the Cyberwomen curricula⁸ and implement safer practices ;)
- Install the Privacy Badger browser plugin⁹

⁶<https://zeptajs.com/>

⁷<https://github.com/y7kim/agency-jekyll-theme>

⁸<https://cyber-women.com/en/#modules>

⁹<https://www.eff.org/privacybadger/>

-
- Configure your Firefox browser to opt out of tracking¹⁰

How do I change my cookie settings?

Most web browsers allow some control of most cookies through the browser settings. To find out more about cookies, including how to see what cookies have been set, visit <https://aboutcookies.org> or <http://www.allaboutcookies.org/>

Find out how to manage cookies on popular browsers:

- Google Chrome¹¹;
- Microsoft Edge¹²;
- Mozilla Firefox¹³;
- Microsoft Internet Explorer¹⁴;
- Opera¹⁵;
- Apple Safari¹⁶.

To find information relating to other browsers, visit the browser developer's website. To opt out of being tracked by Google Analytics across all websites, visit <https://tools.google.com/dlpage/>.

¹⁰<https://support.mozilla.org/en-US/kb/how-do-i-turn-do-not-track-feature>

¹¹<https://support.google.com/accounts/answer/61416?co=GENIE.Platform%3DDesktop&hl=en>

¹²<https://privacy.microsoft.com/en-us/windows-10-microsoft-edge-and-privacy>

¹³<https://support.mozilla.org/en-US/kb/enable-and-disable-cookies-website-preferences>

¹⁴<https://support.microsoft.com/en-gb/help/17442/windows-internet-explorer-delete-manage-cookies>

¹⁵<https://www.opera.com/help/tutorials/security/privacy/>

¹⁶https://support.apple.com/kb/ph21411?locale=en_US