

CWC PRIVACY NOTICE (LONG-FORM) IMPACT AND INSIGHT TOOLKIT

About Counting What Counts (CWC)

We are Counting What Counts Ltd. (**CWC**), a team of consultants and researchers who specialise in impact evaluation and measurement. Our aim is to empower users to better measure and communicate their unique impact and value, building a culture of thoughtful evaluation and data-driven decision making.

Arts Council England (**ACE**) has engaged CWC to develop and manage the Impact & Insight Toolkit (**IIT**) and related services (the **IIT Services**) to provide select National Portfolio Organisations (**NPOs**) with a shared approach to evaluating their work through surveys they create in the IIT, and to sharing certain data and insights with ACE using the self-serve functionality provided within the IIT.

CWC is a data processor to ACE and NPOs for personal data they process using the IIT and IIT Services.

However, we act as a data controller when we process personal data of the individuals within the NPOs who use the IIT and IIT Services (**Authorised Users**), and those that have expressed an interest but have not yet enrolled (**Potential Users**) to administer our business in relation to the IIT and IIT-related services and the Impact and Insights website at <https://impactandinsight.co.uk/> (the **Website**).

About this Privacy Notice

This privacy notice describes how CWC processes the personal data of Authorised Users and Potential Users of the IIT and IIT Services and visitors to the Website (**Website Visitors**).

This does **not** apply to:

- Survey participants: CWC does not process personal data of survey participants for its own purposes. Survey participants should consult the privacy notice of the NPO that issued the survey to learn how they process your personal data when using the IIT and IIT Services.
- NPOs: For personal data CWC processes on your behalf, consult the data processing addendum and other information we provided during registration.
- Website visitors to the www.countingwhatcounts.co.uk website: This privacy notice only addresses the IIT and IIT Services accessed through the Impact and Insights website at <https://impactandinsight.co.uk/>. Visitors to www.countingwhatcounts.co.uk can find information about the personal data we process about them in the privacy notice and cookie widget on that website.

Our Contact Details

Address: 82B High St, Sawston, Cambridge CB22 3HJ

Company number: 09002101 ICO Register of Fee Payers reference number: ZA141427

Privacy Lead: John Knell. Email address: support@countingwhatcounts.co.uk

Phone number: +44 (0) 1223 656 255. Website: www.impactandinsight.co.uk

OUR PRIVACY COMMITMENT

We're committed to keeping your personal data protected and respecting your privacy choices

- We limit what personal data we process to what is necessary and proportionate to meet our legitimate business needs and any applicable legal obligations, making sure the processing is not only lawful, but fair.
- We do what we say we'll do with your personal data. We'll never re-purpose your personal data in ways you wouldn't reasonably expect, unless the law requires us to do so or an exception applies, in which case we will ensure you are informed, subject to any legal constraints.

Unlike many commercially-available survey platforms on the market, we do **not** track individual Website Visitors, Authorised Users or Potential Users to serve targeted ads, create or sell profiles to data brokers or track you across the web. We do **not** use your personal data for profiling or automated decision-making purposes.

Nor do we use your personal data for direct marketing activities, or engage in any data-matching activities or educated guessing techniques like browser fingerprinting to enrich the personal data we hold or identify you against your wishes. In the unlikely event that this changes, we will let you know, and provide you with a simple and effective way to exercise your choices.

The IIT is purpose-built to help NPOs gain data-driven insights to assess the impact of their work. In a similar vein, CWC gathers aggregated analytics – when individuals consent by opting in through our cookie widget – to gain insights and improve user experience of the Website, the IIT and the IIT Services. We apply privacy-preserving techniques from the start in line with ICO guidance (see "Cookies and Analytics").

- We take care when we share your personal data with others who support our work, vetting suppliers for data protection compliance, signing binding contracts to ensure confidentiality and consistent protection of the personal data they process on our behalf, and ensuring our tech stack is designed and configured with a high standard of data protection in mind.

For example, for analytics we use [Matomo](#), a privacy-focused alternative to Google Analytics. So if you opt in to analytics cookies and trackers, you can be confident we remain in control of that data and we are protecting it to a high standard while respecting your privacy choices.

- Where possible, we ensure your personal data remains in the UK or the EEA or is transmitted to countries the UK has determined provide adequate protection. Where an international transfer is required, we make sure we have [Appropriate Safeguards](#) in place, such as Binding Corporate Rules or model contracts approved by UK authorities (International Data Transfer Agreements (**IDTAs**) or their predecessor Standard Contractual Clauses (**SCCs**)).
- We make it easy for you to exercise your rights and preferences, and we respect your choices.
- We keep your personal data secure, up-to-date, and accurate, and only share with those that have a legitimate need-to-know, whether within or outside our organisation.
- We don't process children's personal data nor do we offer or target our IIT or IIT Services to children or minors. Authorised Users must be 18 years or older and attest to this when they agree to our terms. Since the IIT and IIT Services are only available to select NPOs approved by ACE, the likelihood of anyone under 18 years of age accessing the IIT is extremely low. NPOs that register undertake to ensure their Authorised Users are 18 years or older.

THE TYPES OF PERSONAL DATA WE COLLECT AND USE

The types of personal data we capture and use will depend on what you are doing when you access the Website or use the IIT or IIT Services, what you choose to provide, and how and when we engage with you.

We process the following types of personal data about Authorised Users and Potential Users:

- Contact Details: Name, business email address, phone number (optional).
- Contract and Registration Details: The name of the ACE-registered NPO signatory represents, signatory's contact details, title, e-signature, time stamp, confirmation that the signatory and Authorised Users are or will be over 18 years of age.
- Privacy Preferences: e.g. cookie choices, communication preferences). See "Cookies and Analytics", below, for detail.
- Account Details: IIT account permissions or privileges, user ID, NPO.
- Correspondence: details about support requests, queries, complaints, or rights requests, including associated metadata such as time stamps and

read receipts and ID verification where applicable (for Data Subject Access Requests (**DSARS**)), feedback, calls / videoconferencing communications.

- Training Data: training and workshop logs confirming attendance in-person or online (plus data and metadata associated with it, e.g. electronic time stamp, login, user name or display name, etc), questions, comments or reactions in the chat (unless you choose to do so anonymously).
- Usage Data (personal data derived from your interaction with the IIT or IIT Services): login attempts and times; audit trails; cookie data, device data and analytics data. See Cookies and Analytics, below.

See the table below to learn more about how and why we process your personal data, the Lawful Basis (in parentheses) and, where it is transferred outside the UK or EEA, the Appropriate Safeguard. Please Refer to the “Lawful Bases Table” and in “Sharing your Personal Data / International Transfers” section for more detail:

Why and when we use your personal data	How we process your personal data
<p>To respond to a query using our online form or run a survey of Authorised Users or other NPOs</p>	<ul style="list-style-type: none"> • How: Directly from you, using personal data you provide through a survey form powered by Culture Counts, our data processor, who also operates the performance evaluation platform that powers the surveys you’ll create using the IIT. • You will be redirected to a UK instance of the Culture Counts UK website dedicated to these queries and surveys. See this example here. • What we do with it: We’ll use it to communicate with you and process your registration request (Contractual Necessity) and to gather statistics to understand trends so we can improve the IIT Services (Legitimate Interests). • Where? The personal data you provide will be transmitted to our servers in the UK. We will store and access the personal data using our CRM system Pipedrive and communicate with you via email through Microsoft Outlook.

	<p>Appropriate Safeguards are not necessary as Microsoft stores our data in UK data centres and Pipedrive stores our data in Frankfurt, Germany, which the UK has recognised as Adequate.</p>
<p>To communicate with you</p>	<ul style="list-style-type: none"> • How: Using information you've already provided (Contact Details) and the agreed manner of communication you're your Privacy Preferences: via phone (through our respective mobile phone or land line providers), via email (we use Microsoft Outlook), via video conference (using Microsoft Teams, Zoom or your own provider). We also communicate with you about important updates or information related to the service via email or announcement within the IIT. • What we'll do with it: We'll communicate with you in real time and may take notes that we will keep with our records in relation to your account as appropriate (e.g. to document key points discussed or decisions made, or to document a complaint and its resolution) (Contractual Necessity). • Where: This will vary depending on the services used. Note Zoom and Microsoft Teams are global video conferencing platforms. Microsoft stores UK data in the UK, but Zoom is US-based. Appropriate Safeguard for Zoom: Standard Contractual Clauses (Zoom).
<p>To register your NPO and Authorised Users and provide customer service or support</p>	<ul style="list-style-type: none"> • How: You complete and e-sign the contracts package, providing the Contract and Registration Details. You assign an Authorised User (or are assigned Authorised User status) using functionality in the IIT, which will include Contact Details and Account Details. Or you contact us with a support request. • What we do with it: We use this to document our contractual relationship with you, manage your account and provide support (Contractual Necessity).

	<ul style="list-style-type: none"> • Where: Most data is stored on our servers in the UK. Some personal data, notably your Contact Details, may be incidentally transmitted outside the UK to our Australia-based processor, Culture Counts, in the course of providing customer support that requires their technical expertise. Appropriate Safeguard: Standard Contractual Clauses. <p>We use DocuSign as our data processor to automate our contract process and obtain e-signatures. DocuSign is a global company and Contract Details may be transferred outside the UK. Appropriate Safeguard: Binding Corporate Rules for Processors (considered the 'gold standard').</p>
<p>To ensure the IIT functions properly and remains secure</p>	<ul style="list-style-type: none"> • How: By analysing audit and access logs, time stamps, bug reports, etc. and responding to security alerts or suspicious behaviour within the IIT (which generally should not identify you on its own unless additional data is provided). • What we do with it: We analyse the data to trouble shoot any issues. We do not attempt to identify the individual concerned unless necessary to resolve the issue (e.g. if it appears suspicious behaviour is linked to a particular account, we may need to link it back to contact the individual or the NPO to investigate or take action) (Legitimate Interests). • Where: Our AWS server is located in London, however Australia-based Culture Counts staff may incidentally process personal data in the course of providing support, so some very limited amounts of personal data may be transferred outside the UK in such cases. Appropriate Safeguard: International Data Transfer Agreement.
<p>To gather analytics on our website and the IIT</p>	<ul style="list-style-type: none"> • How (if your Privacy Preferences show you consented) : When you interact with the Website or the IIT, for example by downloading

	<p>a document, navigating across pages, clicking on a link, etc.</p> <p>We use Matomo, a privacy-focused analytics tool, to gather and analyze Usage Data. Matomo is our data processor for analytics and never uses this personal data for its own purposes. We remain in full control.</p> <ul style="list-style-type: none"> • What do we do with it: We use analytics to understand how Authorised Users, Potential Users and Website Visitors navigate the https://impactandinsight.co.uk/ IIT so that we can gain insights into what works and what doesn't, what content is popular, and determine ways to optimise user experience. We can compare that to other data, such as aggregated data on support requests and FAQs, to determine whether other interventions or support materials may be required or whether those we have created are meeting Authorised Users' needs. For example, if we create a support document or training video to address an FAQ on sharing evaluations, we expect to see a decrease in support requests or questions on that topic. If there is no decrease, our support material may either be inadequate or too difficult to find. Our analytics help us drill down and trouble-shoot the issue (Consent). • Where: Matomo's servers are located in the EU. Since the UK authorities have determined the EU member states to be Adequate for data protection purposes, no Appropriate Safeguard is needed.
<p>To capture and respect your privacy preferences</p>	<ul style="list-style-type: none"> • How: when you set your Privacy Preferences using our cookie widget (or proceed to navigate the site, in which case the default is set to strictly necessary cookies), when you unsubscribe from receiving messages or adjust your preferences, including preferred method of communication.

	<p>We use Cookiebot by Usercentrics to record and manage cookie consents.</p> <ul style="list-style-type: none"> • What we do with it: Cookiebot stores an anonymous, random and encrypted key value and your consent status in a first-party cookie on your browser for 12 months (unless you delete them earlier). This allows us to prove we've obtained the necessary consents and helps us respect your Privacy Preferences (Legal Obligation). • Where: Cookiebot is based in Denmark, which the UK has recognised as Adequate, so no Appropriate Safeguards are required.
--	---

LAWFUL BASIS TABLE

LAWFUL BASIS	WHAT THIS MEANS
CONSENT	You have given us permission, which you can withdraw at any time. We need your Explicit Consent to process sensitive data like health-related data (Special Data) or to transfer your Personal Data outside the EEA where we don't have another Appropriate Safeguard in place, or for any Automated Decision Making that has significant legal or other effects unless an exception applies. We do not process any Special Data of Authorised Users or Potential Users, nor do we engage in Automated Decision Making.
LEGITIMATE INTERESTS	To help fulfil a legitimate business objective after confirming we've only used what's reasonably necessary and proportionate to meet that objective and struck the right balance between our interests and yours using a Legitimate Interests Assessment.
CONTRACTUAL NECESSITY	To enter into or fulfil our contract with you, including to respond to registration queries or support requests.
LEGAL OBLIGATION	To comply with the law (e.g. tax reporting or legitimate law enforcement requests, court orders, or Freedom of Information Requests where the conditions have been satisfied. We will notify you in

	advance unless the law prohibits us from doing so or it would undermine an investigation).
VITAL INTERESTS	In rare instances where one of the others don't apply but we need your personal data to protect your vital interests or those of another person. It is highly unlikely we would ever need to rely on this Lawful Basis.
PUBLIC TASK	This Lawful Basis applies to processing that is necessary to perform a task in the public interest or for official functions, where the task or function has a clear basis in law. It is most relevant to public authorities, but it can apply to any organisation that exercises official authority or carries out tasks in the public interest. We don't currently rely on this Lawful Basis. As we operate the IIT and IIT Services on behalf of ACE to help funded NPOs evaluate the impact of their work, there may be rare instances where it might apply, for example to respond to a <i>Freedom of Information Act</i> request. We recommend you contact ACE for more detail on this Lawful Basis.

SHARING YOUR PERSONAL DATA / INTERNATIONAL TRANSFERS

Like most businesses, we rely on a range of external parties to support our work, and tech providers in particular. Before entrusting your personal data to these recipients, we vet their practices to ensure we're confident they'll provide adequate protection, and enter into legally-binding agreements to make sure those that process personal data on our behalf commit to taking the necessary care and acting on our instructions.

Some of our tech providers or service providers are located outside the UK or EEA in countries that have not yet been recognized as Adequate by UK authorities. In such cases, we ensure Appropriate Safeguards are in place in line with requirements set by UK GDPR and ICO guidance. The table below provides more detail.

Company (Click for more information)	Data Shared	Purpose	Where Located (Appropriate Safeguard)
Amazon Web Services (AWS) (Sub-Processor)	<ul style="list-style-type: none"> Contact Details NPO Details 	A cloud hosting service we use to accelerate our website and a	London

	<ul style="list-style-type: none"> • Contract and Registration Details • Account Details 	storage service (Amazon Simple Storage (S3))	
Culture Counts (CC) (Sub-Processor)	<ul style="list-style-type: none"> • Contact Details • NPO Details • Contract and Registration Details • Account Details • Correspondence • Usage Details (for the IIT) 	CC powers the IIT, providing user credentials and technical support and maintenance	Australia (International Data Transfer Agreement)
Matomo (Sub-Processor)	<ul style="list-style-type: none"> • See "Cookies, Statistics and Analytics" below. We remain in full control of this data. 	A privacy-preserving analytics tool EU authorities such as the EDPS also use due to its compliance with strict data protection rules.	EU
Microsoft Office 365 (Teams, Outlook, Word) (Sub-Processor)	<ul style="list-style-type: none"> • Contact Details • Correspondence 	A productivity cloud we use to communicate with you.	UK
Zoom (Sub-Processor)	<ul style="list-style-type: none"> • Contact Details • Correspondence 	A video conferencing app we use to communicate with you.	US (Standard Contractual Clauses)
Arts Council England (ACE) (Controller / Recipient)	<ul style="list-style-type: none"> • Contact Details • Correspondence (e.g. to resolve queries or issues) 	ACE offers the IIT to NPOs as part of their funding agreement and requires certain information in identifiable (e.g. who from the NPO is registered) and aggregate form (e.g. number of NPOs registered) as described in	UK

		the registration package	
Cookiebot (aka Cybot) by Usercentrics (<i>Sub-Processor</i>)	<ul style="list-style-type: none"> • IP number in anonymized form (last three digits are set to '0') • The date and time of the consent (for retention periods) • User agent of your browser • URL from which the consent was submitted. • An anonymous, random and encrypted key value. • Your consent state, serving as proof of consent 	Cookiebot is a consent management platform that makes it easier for us to automatically manage cookie consents on our website	Denmark
Pipedrive (<i>Sub-Processor</i>)	<ul style="list-style-type: none"> • Contact details • Correspondence • NPO details • Contract and Registration details • Account details • Correspondence • Training data 	A customer relationship management software we use to help us manage our client relationships more efficiently and effectively. Learn more here .	Frankfurt, Germany

RETENTION PERIODS

We'll generally retain your personal data as long as a business relationship exists with you or until you ask to be removed from our system, unless we have a legal obligation to retain it longer. We stop actively using your personal data once a retention period has been reached. Thereafter, we delete, anonymise or archive certain personal data elements as described below.

Personal Data Elements	Retention Period	Action
Contact details, NPO details, Contract and Registration details,	<p>Authorised Users: The duration of our contractual relationship and for an additional 6 years post-termination.</p> <p>Potential Users: up to 12 months.</p>	Archive 6 months post termination. Delete 6 years post-termination.
Account details	Authorised Users: For the duration of our contractual relationship or one year since the date of last login, whichever is earlier (inactive accounts).	Archive 6 months post-termination. Delete 3 years post-termination.
Correspondence	<p>Support requests (where not anonymous): 6 months from date of resolution.</p> <p>Feedback (where not anonymous): 1 year from date provided, unless it is a testimonial (retained up to 3 years unless you request deletion sooner).</p> <p>Complaints DSARs: Up to 6 years from date of DSAR resolution or post contract termination (for complaints).</p>	<p>Archive upon resolution.</p> <p>Archive in anonymised form.</p> <p>Archive once resolved then destroy after 6 years.</p>

<p>Usage Data</p>	<p>For security: We take measures to limit what data can be linked to you upon collection. Thereafter we aggregate and anonymise the data up to 6 months from the last action, unless a security or privacy incident is associated with it, in which case we retain it up to 3 years from resolution or close of investigation.</p>	<p>Anonymise and archive in anonymised form (if no incident). Archive (if there is an incident).</p>
<p>Usage Data</p>	<p>For analytics: We take measures to limit what data can be linked to you upon collection. Thereafter we aggregate and anonymise the data (within 3 months of collection).</p>	<p>Aggregate upon collection, then anonymise.</p>
<p>Privacy Preferences</p>	<p>Cookie consents: 12 months from time on time and date stamp, unless you clear your browser cookies sooner, in which case you'll be asked for consent again.</p> <p>Marketing preferences (e.g. unsubscribe): indefinitely.</p> <p>Communication preferences for service messages: duration of</p>	<p>Delete on expiry and request fresh consent upon subsequent visit.</p> <p>Indefinite to satisfy a Legal Obligation to maintain a suppression list.</p> <p>Once account is flagged as inactive or contract has terminated, this information is archived</p>

	relationship and up to 1 year from either contract termination or last date of activity (whichever is earlier).	for 1 year and then deleted.
--	---	------------------------------

HOW WE KEEP YOUR PERSONAL DATA SECURE

We have implemented appropriate information security policies and procedures in line with ISO 27001 and the Cyber Essentials framework including:

- Procedures to regularly review data access rights and our sharing practices
- Procedures for the secure disposal of data, media and equipment
- Procedures to regularly review our risk exposure and table appropriate mitigations that consider possible impact on customers and end-users, best practice solutions, and resource availability

Internal Data Protection and Information Security policy documents are updated as the law evolves and employees receive training to ensure they understand their data protection obligations. All information passed between you and CWC when using our online services is sent using secure industry standard encryption.

Your rights under applicable data protection law

You have the following rights with respect to your personal data, provided the criteria are met:

- The right to be informed about our processing of your personal data
- The right to have your personal data corrected if it's inaccurate and to have incomplete personal data completed
- The right to object to processing of your personal data
- The right to restrict processing of your personal data
- The right to have your personal data erased (the "*right to be forgotten*")
- The right to request access to your personal data and information about how we process it
- The right to move, copy or transfer your personal data

Learn more about your rights [here](#).

To exercise your rights, please contact our Privacy Lead, John Knell, via email at support@countingwhatcounts.co.uk.

COMPLAINTS

We hope that you won't ever need to, but if you do want to complain about our use of personal data, please send an email with the details of your complaint to support@countingwhatcounts.co.uk . We will investigate and respond to all complaints we receive.

You also have the right to lodge a complaint with the Information Commissioner's Office ("ICO") is the UK data protection regulator/supervisory authority. For further information on your rights and how to complain to the ICO, please refer to the [ICO website](#).

CHANGES TO THIS PRIVACY STATEMENT

We'll notify you if there are any material changes to this Privacy Notice as required by applicable law or where we intend to process your personal data for a new purpose before we start that new processing activity.

LINKS TO OTHER WEBSITES

Certain hypertext links or social sharing buttons in this website may lead you to websites which are not under the control of Counting What Counts Ltd. When you activate these, you may leave our website. These links are provided solely for your convenience and do not represent any endorsement or recommendation by Counting What Counts Ltd. We accept no responsibility or liability for the contents of any website to which a hypertext link exists and gives no representation or warranty as to the information on such websites. We encourage you to read their privacy notices to learn more about their data protection practices.

COOKIES, STATISTICS AND ANALYTICS

Cookies and Similar Technologies

Cookies are small text files placed on your computer, smartphone or other device and are commonly used on the internet. We use cookies and similar technologies to:

- collect information that will help us understand visitors' browsing habits on the Website, and compile statistical reports on website / IIT activity for Authorised Users, Potential Users and Website Visitors who provide their opt-in using our cookie widget (Consent), e.g. number of visitors and the pages they visit
- remember information about you when you visit our site (preferences, choices). We may need to do this to provide some of our services if you provide your consent, e.g. if you use the 'Remember me' option on the login
- to remember your cookie preferences selected using our cookie widget (Legal Obligation).

We use Cookiebot by Usercentrics (a trademark of Cybot), a Danish company, to capture and manage cookie consents. By default, our website is set to only capture strictly necessary cookies, however you may use the Cookiebot cookie widget to opt in to other types of cookies and technologies, for example to manage your preferences, enhance performance or enable us to gather analytics about our website.

When you set your preferences, Cookiebot securely transmits your choices and additional data required to help us record and manage it:

- Your IP number in anonymized form (last three digits are set to '0').
- The date and time of the consent (to manage retention periods)
- User agent of your browser
- The URL from which the consent was submitted
- An anonymous, random and encrypted key value (**Key**)
- Your consent state, serving as proof of consent

The Key and consent state are also saved in your browser in the first party cookie "CookieConsent" so that the website can automatically read and respect your consent on all subsequent page requests and future sessions for up to 12 months. The Key is used for proof of consent and an option to verify that the consent state stored in your browser is unaltered compared to the original consent submitted to Cybot.

You will find a detailed list of the cookies we use, how long we retain the cookie data and the recipients (if applicable) that receive data we capture using cookies

in our Cookiebot cookie widget and change your settings at any time by ticking or unticking the relevant boxes.

You may need to refresh your page for your settings to take effect.

Alternatively, you can control cookies through your browser settings.

Find out how to manage cookies on popular browsers:

- [Google Chrome](#)
- [Microsoft Edge](#)
- [Mozilla Firefox](#)
- [Microsoft Internet Explorer](#)
- [Opera](#)
- [Apple Safari](#)

To find information relating to other browsers, visit the browser developer's website.

Learn more about cookies at www.aboutcookies.org or www.allaboutcookies.org.

Analytics

We use a privacy-preserving analytics tool called [Matomo](#) – which many [EU authorities](#) use to ensure compliance with strict privacy and data protection rules - to analyse how Authorised Users and Potential Users interact with the Website.

We aim to provide the best possible user experience to help the arts and cultural communities get the most out of their data. We're interested in the bigger picture so we can find out what works, and what doesn't, as we constantly strive to improve the user experience. We generally anonymize or aggregate the personal data at source, e.g. through IP anonymization and have taken other steps as outlined [here](#) to increase privacy protection by reducing the ability to link this data back to you. We process the following data elements using Matomo, most of which are anonymous or pseudonymous:

- User IP address (anonymized)
- Optional User ID
- Date and time of the request
- Title of the page being viewed (Page Title)
- URL of the page being viewed (Page URL)
- URL of the page that was viewed prior to the current page (Referrer URL)
- Screen resolution being used

- Time in local user's timezone
- Files that were clicked and downloaded (Download)
- Links to an outside domain that were clicked (Outlink)
- Pages generation time (the time it takes for webpages to be generated by the webserver and then downloaded by the user: Page speed)
- Location of the user: country, region, city, approximate latitude and longitude (Geolocation) to preserve privacy (Exact location is never used)
- Main Language of the browser being used (Accept-Language header)
- User Agent of the browser being used (User-Agent header)
- From the User-Agent, we use Matomo's Universal Device Detection library to detect the browser, operating system, device used (desktop, tablet, mobile, tv, cars, console, etc.), brand and model.

Some information is also stored in first party cookies and then collected by Matomo:

- Random unique Visitor ID
- Time of the first visit for this user
- Time of the previous visit for this user
- Number of visits for this user