**Mozilla Vendor Privacy Review**

**NOTE: Please make sure to include your product team, technical team, privacy team and your legal team in this review - ourselves and our users will be relying on it.**

Here are some things you should know about us:

We are different: Mozilla is a non-profit dedicated to putting the user in control and shaping the future of the Web for the public good. Our users are extremely important to us, as is their trust, and a very important part of how we select vendors is their ability to treat our user data properly.

Six core privacy principles guide our data practices and operations at Mozilla. These principles stem from the [Mozilla Manifesto](http://www.mozilla.org/about/manifesto).  We apply these six principles when selecting trusted vendors.

1. **No Surprises:** Only use and share information about our users for their benefit and as spelled out in our notices.
2. **Limited Data:** Collect and retain the least amount of user information necessary and share data anonymously whenever possible.
3. **Real Choices:** Educate users at the point that we collect any data and give them the option to opt out whenever possible.
4. **User Control:** Innovate, develop and advocate for privacy enhancements that put users in control of their online experiences.
5. **Sensible Settings:** Establish default settings that balance safety and user experience appropriately for each transaction.
6. **Trusted Third Parties:** Make privacy a key factor in selecting and interacting with partners.

Some things you should know about how we think about data that may be different than you are used to being asked by other clients:

We consider “Mozilla Data” to be all data collected by you in providing us services, including aggregate data and IP address. We may be ok with you doing certain things with aggregate data, but need to know exactly what that is and describe it in detail in the agreement.

We consider IP address to be potentially personally identifiable and expect you to have a data retention policy for all the data you collect, including IP logs.

If you are collecting any data from us or our users for targeting advertisements or marketing, we will need to talk about how your system works, your opt-out or opt-in choices for end users, and our options for whether or not we can turn that feature off.

See next page for questionnaire. Please submit written answers to stacy@mozilla.com.

Please provide written answers to the following questions. As noted earlier, be sure to include your **product team, technical team, privacy team** and your **legal team** to help ensure the accuracy of your answers.

|  |  |
| --- | --- |
| **Questions** | **Answers** |
| Have you read Mozilla’s privacy policy and compared it to your own?  Are there any significant differences and if so, how would you resolve? | Experientia is compliant with Mozilla’s privacy policy. We do not share collected information with any other service provider. We collect data through qualitative methods and use these data to provide our client with analytical insights. Data are not made public for any reason, as per Italian privacy legislation. |
| Do you have a process to notify Mozilla if you make any changes that could cause Mozilla to violate its privacy policy? | Experientia always asks its client for explicit permission any time and for any reason that we are requested to reveal the collected data by a legal authority. |
| Are you willing to acknowledge that Mozilla and/or its users own all right, title, and interest in and to Mozilla data (i.e. data collected, stored or otherwise processed on behalf of Mozilla, whether by us or you) | This is consistent with Experientia’s privacy policy. We hereby acknowledget that Mozilla and/or its users own all right, title, and interest in and to Mozilla data (i.e. data collected, stored or otherwise processed on behalf of Mozilla, whether by them or us, insofar compliant with Italian privacy legislation Mozilla will be responsible for the usage of data collected by Experientia on Mozilla’s behalf. |
| Do you have processes in place to limit processing (collection, use, or disclosure) of Mozilla data to what is expressly permitted in a written agreement? | Experientia asks for signatures on release forms to all participants in the research fieldwork. When required we ask participants to sign release forms that limit the usage of collected data to the project purposes only and that explicilty state the limitations to data processing. |
| Is your service offered from a Mozilla domain, or is it a hosted service? Can you use a Mozilla domain name? (ex: for cookies) | We will not use online services, but only our own company server. If we are required to adopt research methods that imply the hosting of services, we can use a Mozilla domain name. |
| **Data use:** |  |
| Do you plan to use Mozilla data, whether in aggregate or individual form, for any purposes other than providing us with services? (For example, use in targeting advertising or marketing, reporting / analytics, communications, etc.) Please describe in detail and specify whether aggregate or individual data. | We collect only qualitative data, mostly in individual forms for research purposes. We never use collected data for advertising or marketing purposes. This is also not allowed by Italian legislation, unless explicit consent has been given by the participant. |
| If yes, how do you plan to make the purposes of such use clear to the user and is the user able to opt-in or opt-out? | Not applicable |
| **Data storage:** |  |
| Can Mozilla’s data be stored separately from your other customers? | We collect qualitative research data in separate forms. We never combine data from different projects or use data from one project in another project. We store project data in client-specific containers in our internal digital archive. There is no risk of them being confused or contaminated. |
| Do you have processes in place to avoid correlating or aggregating Mozilla data with any other data? | See above |
| **Data retention:** |  |
| How long do you plan to retain Mozilla data? If you store different types of data for different amounts of time, please describe those amounts for each kind of data. | Experientia keeps the qualitative data in an internal digital archive which is protected and cannot be accessed. In theory those data are never deleted, unless the client asks us to do so. |
| Do you have processes in place to destroy or return Mozilla data upon written instruction from Mozilla?   | Yes, we do. Data in our digital archives can be deleted upon written request. |
| **Data collection: (if applicable)** |  |
| What data elements do you plan to collect in connection with the service you are providing to Mozilla? Please list both Non-PII data as well as PII. | Experientia collects only qualitative PII in digital formats. These data are:* interview data
* participatory workshop data
* ethnographic data
* visual data
 |
| What data elements are collected/transmitted from a Mozilla domain as a result of your service? Is there a way for users to opt-out? | Not applicable to Experientia’s services. |
| Do you collect any sensitive data? (ex: birth date, credit card information, medical data, etc.) | Experientia usually collects only very basic personal data, like birth date and marital status. Information on more sensitive topics, such as personal health or finances, is usually derived from general sources (such as belonging to a category or range in a set). |
| Is the data you collect absolutely necessary to provide the service? If not, list pieces of data you are collecting that are not necessary. | Experientia does not generally collect data that are out of the scope or focus of the qualitative research being conducted. |
| Are there any users who might be unaware that you are collecting their data? For example, do you receive any data from users who may not be using your service? | Not applicable to Experientia’s services. |
| **Tracking technologies** |  |
| Does your service enable you to track users on a Mozilla domain? | Not applicable to Experientia’s services. |
| What technologies will be used in collecting user data (ex: hardware, software, application, cookies, web beacons, Flash, Locally Stored Object [Flash cookies, HTML cookies], ajax, etc.)? | Experientia uses only typical video and audio recording instruments, and research participants first sign a release form agreeing to be recorded. |
| Do you do any tracking across sites? | Not applicable to Experientia’s services. |
| **Viral Sharing:** |  |
| Do you offer any viral sharing features, such as email tell a friend functionality, Facebook, or Twitter share buttons? | Not applicable to Experientia’s services. |
| If you offer sharing features, do you track their use and what information are you collecting when you track? | Not applicable to Experientia’s services. |
| If email tell a friend functionality, do you limit the use of the information collected? | Not applicable to Experientia’s services. |
| **Rules and Regulations:** |  |
| What processes do you have in place to comply with all applicable federal, state, local and international privacy, data protection, and security laws, rules and regulations?   | Experientia is a legal entity that acknowledges the most common international privacy framework, like that provided by OECD (see <http://oecdprivacy.org/>), as well as the stringent Italian privacy legislation. |
| Do you transfer personal data between the US and the European Union (EU)? | No |
| Are you EU Safe Harbor certified? | Not applicable |
| Are you PCI certified? (if applicable) | Not applicable |
| Do you participate in any privacy seal programs? (ex: TRUSTe) | No |
| Are you aware of any regulator investigations, actions or lawsuits against you that are related to data privacy?  | No |
| **Notice & Communications: (if applicable)** |  |
| Do users receive clear notice prior to receiving any communications from you? If so, how? | Experientia has a recruitment process in place through which people involved are informed about the research processes and the general objectives. |
| If you collect user data directly, how are users informed about it? | Users are always participants in a research process, and sign release forms and agree to participate in the study. Researchers explain research aims and methods thoroughly prior to commencing. Data is collected directly from users through interviews, contextual observation and tests. |
| Is data use limited to what is described? | Yes, always. |
| Can you accommodate a Mozilla privacy notice? | Yes, we can accommodate any particular requests from Mozilla within the research participants’ release forms. |
| Do you send any communications (ex: email) directly to users? If so, how do you make users aware of the types of communications they can expect to receive? Can they opt-in/out? | Once the research period is over, participants receive no further communication from Experientia. At the start of the fieldwork, participants are informed of any ongoing research-related communication they may receive, and the means of communication which will be used. All communication is strictly related to the relevant research study.Selected participants in the fieldwork research can opt-out at any moment, if they wish to do so. |
| **Employees and Subcontracting:** |  |
| What type of background screening do you conduct for employees and/or contractors with access to client user data? | Experientia employees and subcontractors are always bound by non-disclosure and non-competitiveness policies and contracts and to the same privacy and data protection legislation mentioned above. |
| Do you use any subcontracting resources? (i.e. vendors or contractors who provide some of the services Mozilla is requesting) | Sometime Experientia uses local facilitators and translators for the languages that we cannot master in house. |
| Do you have processes in place to obtain written consent for any subcontracting that would involve Mozilla data? | Yes. Experientia asks for consent forms and NDA to be signed by subcontracting agents/resources. |
| Are any subcontractors bound by written agreement to handle the data according to the requirements in the client contract? | Yes. All subcontractors who handle research data are bound by the requirements in the client contract.  |