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. 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?	Yes No
Do you have a process to notify Mozilla if you make any changes that could cause Mozilla to violate its privacy policy?	Yes
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)	Yes
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?	Yes
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.	No
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?	N.A.
Data storage:	
Can Mozilla's data be stored separately from your other customers?	Yes
Do you have processes in place to avoid correlating or aggregating Mozilla data with any other data?	Yes
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.	We usually store the data till we close our company year-end financial books, after which, we will archive the data for another 3 years in case of auditing questions.
Do you have processes in place to destroy or return Mozilla data upon written instruction from Mozilla?	We can return the data to Mozilla upon request from Mozilla after the close of the event.

Data collection: (if applicable)	N.A.
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.	IP Address logs? Y/N PII: Non-PII data:
Do you collect any sensitive data? (ex: birth date, credit card information, medical data, etc.)	
Is the data you collect absolutely necessary to provide the service? If not, list pieces of data you are collecting that are not necessary.	IP Address logs? PII: Non-PII:
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.)?	
Viral Sharing:	
Do you offer any viral sharing features, such as email tell a friend functionality, Facebook, or Twitter share buttons?	No
If you offer sharing features, do you track their use and what information are you collecting when you track?	No
If email tell a friend functionality, do you limit the use of the information collected?	No
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?	N.A.
Do you transfer personal data between the US and the European Union (EU)?	N.A.
Are you EU Safe Harbor certified?	N.A.
Are you PCI certified?	N.A.
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
Communications: (if applicable)	N.A.
Do users receive clear notice prior to receiving communications from you?	

How do users receive this notice?	
Does the notice clearly describe how the data collected will be used?	
Is data use limited to what is described?	
Can you accommodate a Mozilla privacy notice?	
Employees and Subcontracting:	
What type of background screening do you conduct for employees and/or contractors with access to client user data?	All staff/ contractors handling user data will have to sign a non-disclosure letter with World Express.
Do you use any subcontracting resources? (i.e. vendors or contractors who provide some of the services Mozilla is requesting)	We work with our regular vendors; Printing, Audio Visual and transportation company to provide the printing/publication, audio visual and transportation services. All these services will be handled by World Express Staff, and these vendors will just execute the services required during the event.
Do you have processes in place to obtain written consent for any subcontracting that would involve Mozilla data?	Likewise, we have a non-disclosure letter for vendors to adhere to if the service involves private data.
Are any subcontractors bound by written agreement to handle the data according to the requirements in the client contract?	N.A.