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.

<u>Here are some things you should know about us:</u>

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.

<u>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:</u>

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 SIGNIFICANT DIFFERENCES.
Do you have a process to notify Mozilla if you make any changes that could cause Mozilla to violate its privacy policy?	N/A
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?	PDQ PRINTING WILL NOT COLLECT DATA.
Is your service offered from a Mozilla domain, or is it a hosted service? Can you use a Mozilla domain name? (ex: for cookies)	

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.

DESTROY IMMEDIATELY AFTER USE.

Do you have processes in place to destroy or return Mozilla data upon written instruction from Mozilla?

YES.

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.

N/A — ONLY DATA SENT TO PDQ PRINTING BY MOZILLA WILL BE USED, ✳

IP Address logs? Y/N

PII:

Non-PII 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?

N/A

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:

N/A

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?

N/A

Tracking technologies

Does your service enable you to track users on a Mozilla domain?

N/A

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.)?

N/A

Do you do any tracking across sites?   *N/A*

Viral Sharing:

Do you offer any viral sharing features, such as
email tell a friend functionality, Facebook, or   *N/A*
Twitter share buttons?

If you offer sharing features, do you track their
use and what information are you collecting   *N/A*
when you track?

If email tell a friend functionality, do you limit   *N/A*
the use of the information collected?

Rules and Regulations:

What processes do you have in place to comply   *COMPANY SOP*
with all applicable federal, state, local and   *AND COMPLIANCE*
international privacy, data protection, and   *MANUAL.*
security laws, rules and regulations?

Do you transfer personal data between the US   *N/A*
and the European Union (EU)?

Are you EU Safe Harbor certified?   *N/A*

Are you PCI certified? (if applicable)   *N/A*

Do you participate in any privacy seal   *N/A*
programs? (ex: TRUSTe)

Are you aware of any regulator investigations,
actions or lawsuits against you that are related   *NO*
to data privacy?

Notice & Communications: (if applicable)

Do users receive clear notice prior to receiving   *N/A*
any communications from you? If so, how?

If you collect user data directly, how are users   *N/A*
informed about it?

Is data use limited to what is described?   *N/A*

Can you accommodate a Mozilla privacy   *YES.*
notice?

Do you send any communications (ex: email)
directly to users? If so, how do you make users   *N/A*
aware of the types of communications they can

expect to receive? Can they opt-in/out? *N/A*

Employees and Subcontracting:

What type of background screening do you
conduct for employees and/or contractors with
access to client user data?

CRIMINAL BACKGROUND, FEDERAL EMPLOYMENT/ SOCIAL SECURITY ELIGIBILITY.

Do you use any subcontracting resources? (i.e.
vendors or contractors who provide some of the
services Mozilla is requesting)

NO.

Do you have processes in place to obtain
written consent for any subcontracting that
would involve Mozilla data?

YES.

Are any subcontractors bound by written
agreement to handle the data according to the
requirements in the client contract?

N/A