Body & Data's Data Use Guideline for Newsletter and Website

This document is last updated on 16th March, 2020 which explains the data use guideline of Body & Data in relation to its quarterly newsletter and website. For further clarification on Body & Data and privacy, please refer to privacy policy of the organization.

ABOUT BODY & DATA

Established in 2017, Body & Data works to enhance understanding and access to information on digital rights among women, queer people and marginalized groups where they are able to exercise their rights in a safe and just digital space. We work towards the vision of accessible, safe and just digital space for all, through cross movement building, facilitation for access to information, knowledge building and dissemination on digital rights in the context of Nepal

ABOUT TECH INFRASTRUCTURE OF BODY & DATA

For communication purposes, Body & Data has quarterly newsletter that is sent four times every year. The newsletter generally consists of issues around digital rights in Nepal, work and activities of the organization in that specific quarter and any opportunity or readings around digital rights.

For the newsletter, Body & Data has a self-hosted server, which means that we have autonomy and control over the data and information that is stored in our server - through communication via emails or information used for newsletter purposes.

For the newsletter specifically, we use "MailTrain", an open-source and safe software installed and administered on our server. Open-source means that the code of the MailTrain is openly available to the users and is transparent in terms of the design, safety features and more.

For website, Body & Data uses Wordpress. Body & Data has not made any specific modification to what Wordpress collects by default. [Here is more information about how Wordpress collects your data](#).

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. In case of Nepal, there is no available data protection laws and mechanisms in place. However, the right to privacy is assured by the constitution of Nepal 2015.

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.

BODY & DATA'S COMMITMENT TO PRIVACY

Beyond complying certain minimums, this platform, in its 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.

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.

At Body & Data, our Data Use Guideline is an extension of our values as an organization: an opportunity to learn about our right to privacy, how it can be taken into account and what specific measures we can apply.

For the newsletter specifically, we have had prior process of asking for individuals' consent to receive newsletter from us. The individuals who have agreed to receive the newsletters can unsubscribe at any point of time, without any repercussions.

WHAT WE ARE DOING?

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.

Body & Data, through MailTrain can collect data and information such as whether you have opened our newsletter and have clicked any specific links. However, this information is anonymized and we can't identify you. The data around you reading the newsletter is collected to check and monitor the effectiveness and things that need to be improved in the newsletter.

With specific to our website, we are collecting data and information about how many people have visited a specific web page. The collection of this data is to monitor and evaluate our work – specially in regards to how our publications and research has been read by our audience and been useful. We also use it to get the general understanding of what type of blog posts have more readers, to be able to understand the interest around digital rights, specially within our readers. These data and information are anonymized and Body & Data doesn't try to identify the users.

Communications

Body & Data implements digital security measures when engaging in communication. For communication with the communities, we work with - women, queer folks, tech persons, activists and individuals who are interested in digital rights issues of Nepal. Our communication means are mostly through social media (Twitter, Instagram, Facebook and YouTube), website, signal groups, emails and newsletters.

Communication through emails and newsletters include the security and privacy measures mentioned above as these communication platforms are run through self-hosted channels. Communication via our website happens through email account communication@bodyanddata.org. All e-mail accounts are also

administered by Body & Data. The communication with communities, participants of our workshops and ally activists and organizations happening through signal is encrypted. The communication happening through social media are susceptible to privacy concerns of the specific social media platforms that are used. However, the communications are guided through the values of privacy of the organization and necessary digital security measures are applied.

CHANGES TO THIS GUDIELINE

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

CONTACTS

All questions related to the Data Use Guideline can be sent to the email: communication@bodyanddata.org

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 an 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 making your privacy vulnerable.

- Implement safer privacy practices ;)
- Install the Privacy Badger browser plugin
- Configure your Firefox browser to opt out of tracking.

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 Chrome**;
- **Microsoft Edge**;
- **Mozilla Firefox**;
- **Microsoft Internet Explorer**;
- **Opera**;
- **Apple Safari**.

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 **tools.google.com/dlpage/**.