New EU data protection law in relation to Tiki

Table of contents
- New EU data protection law in relation to Tiki
  - How does this translate for our websites
    - Personal data collection
    - Cookies
    - Summary of action points
  - Various related discussions

New EU data protection law in relation to Tiki

The General Data Protection Regulation (GDPR) (EU) 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union. It addresses the export of personal data outside the EU. The GDPR aims primarily to give control to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.

It was adopted on 27 April 2016. It becomes enforceable on 25 May 2018, after a two-year transition period. The GDPR replaces the 1995 Data Protection Directive.

Because GDPR is a regulation, not a directive, it does not require national governments to pass any enabling legislation and is directly binding and applicable.

(taken from wikipedia)

GDPR in English (and in general)
RGPD in French
DSGVO in German

We got to a lawyer who specializes on such topics and also understands open-source for clarifications about how it applies to the Tiki Software Community Association (TSCA)'s infrastructure servers. Meaning all the *.tiki.org servers.

So, it is about our websites and the data the websites collect and process.

Note that since this is so new, there are obviously no precedents.

What we are not concerned with:

- Nothing related to our mailboxes or mail redirects tiki.org since it's among ourselves.
- The devel and cvs and other mailing lists which are provided by SourceForge are not TSCA's responsibility.

First of all, the Tiki community likes the EU data protection law, so even if the TSCA is registered in Canada, we would like to comply.

Also, if Tiki has everything the TSCA needs for being in compliance, EU users of Tiki can also use Tiki and be compliant.

How does this translate for our websites

Personal data collection

We do not need to volunteer info to anyone any more. Instead, we keep track of proof that we comply in case there is some complaint which prompts
• Our websites need to have a Terms & Conditions' (T & C) page (Mentions "légales" if we want to translate in French which we don't). That's supposed to explain what we do with personal data we collect. Well, in our case it's personal info people volunteer.
• When people create an account (registration), we need to tell them the purpose of this data collection, meaning what we will do with the info they provide. Also they need to accept this and we need to keep track that they accepted.
  ○ We probably don't need to keep track that they accepted for old accounts, as long as we keep proof that these accounts were created before.

Concretely, we need to explain in short form on the registration page and in long form in the T & C page that the info people provide in their user account is visible on the Tiki sites but we don't sell it of give it away to other organizations or companies. Plus, we need some checkbox which is mandatory and configured as "immutable" or some similar thing which prevents users from changing it afterwards.
• Same for the data people provide in the Consultants list.
While we are at it, the consultants list should be a one-year registration which consultants should renew every year (they should get a reminder email), otherwise the entry is deleted, so we don't display uninterested or even dead people.
• People need to be able to correct and edit their personal info.
Nothing to change here, we already do that
• People need to be able to delete their account, meaning all their user info. We can still keep track of their edits in page histories and posts and such through their nickname.
This is usually easy to set up, but for our special situation of using InterTiki logins, some mechanism needs to be devised so user records which are deleted on tiki.org are also deleted from all other *.tiki.org sites.

Cookies

For what it's worth, the current law which still applies says that cookies we need for the purpose of our own technical reasons are OK and unconcerned with the obligation to inform people. Only third party cookies need approval. Not the *.tiki.org ones.

Summary of action points

Right now I see some action points

• Add a checkbox on the registration (account creation) and the consultants tracker
• Write a T & C page
• Write a one-line summary of the T & C, or link to it on the registration template and the consultants template
• Figure out a way of letting people delete their account (or maybe a form for asking for said deletion and we can ask why they want to?)

Various related discussions

> Here is another question. If consent is a legal requirement then in order to accept consent the user will need to qualify under Age of Majority. So maybe our policy should stipulate that one needs to be of Age of Majority or if the user is a minor that only a legal guardian may accept the required consent. I am guessing that would also be the case with Power of Attorney. I presume that we need to do a little due-diligence in establishing that the user is able to give legal consent if consent is a legal requirement.

The lawyer told me it's a widespread issue which does not have any known good practical solution. So she told me the usual way of dealing with this is to mention in the T&C something like: they can't create an
account below 13, and need parental approval from 13 to 17. But your phrasing is less country-dependent 😊
Yes, I know... not a good solution, but the best we can have as far as she knows.

> Question, will they even open an investigation against a Canadian company?

I believe you are correct. In case of a complaint, we are not expected to hand the personal data over but we are supposed to explain our policy about correctly protecting personal data and how we have processes to ensure the people who actually handle the data follow these policies.
In our situation, the European people managing personal data on our servers are assumed to do all that under the responsibility of the Tiki Software Community Association.

So yes, they have to raise the issue in front of the TSCA which is in Canada.

Torsten's summary
Two major points I see with the GDPR are as follows:

1. The GDPR weights up on the best interests and legal rights of both, the person who submits personal data and the recipient/processor/possessor of the data

So personal data has always be treated legitimately, in good faith and trust, transparently and confidentially (transparent from the perspective of processes and regarding the person who originally "owns" or submitted his/her data and confidential towards third party)

2. There is data and circumstances where personal data not necessarily has to be deleted, because the possessor has a legitimate right to possess and to keep the data.

Imagine billing and delivery addresses, email-threads, banning list against spammers, etcetera.

There have been, there are and there will be conflicts, which data is to be kept legitimately and which data is to be deleted. I assume the amount of claims and assessments will be rising - at least for a while - but I think that the good effect is a rising awareness on data protection in general and on individual rights in specific.

The less data we collect, the least locations we use to collect and to store the personal data we need, the most we anonymize upfront (ex Analytics), the more we are on the save side.

I think, the most important thing is to be aware of data protection and to do our best respect and to protect user data and to respect data economy.

Aliases
GDPR