GDPR for OSM

Kathleen Lu
OSMF Legal/Licensing Working Group

Agenda

- Preface
- GDPR 101
- OSMF’s Response
- What’s Next
- Questions
-
-
-

Preface

- GDPR is an EU privacy law
- GDPR is very very complicated
- It is difficult to comply with
- The penalties can be very bad
-
-
-

Before May 25

a survey of over 1,000 companies conducted by the Ponemon Institute in April, half of the companies said they won't be compliant by the deadline. When broken down by industry, 60 percent of tech companies said they weren't ready.

This is, in some ways, an inevitable outcome. A year ago, 61 percent of companies had not even started GDPR implementation. Straight says that, on the whole, European companies — especially those in countries like Germany and the UK, where there are preexisting privacy laws that overlap with GDPR — have had a better time adjusting. (Still, a survey in January of this year found that a quarter of London businesses didn't even know what GPDR was.)

No Easy Solutions

The world's 500 biggest corporations are on track to spend a total of $7.8 billion to comply with GDPR, according to consultants Ernst & Young. Businesses must appoint someone in the protection officer" responsible for compliance. Microsoft Corp. has 300 engineers working to ensure its software is GDPR-compliant.

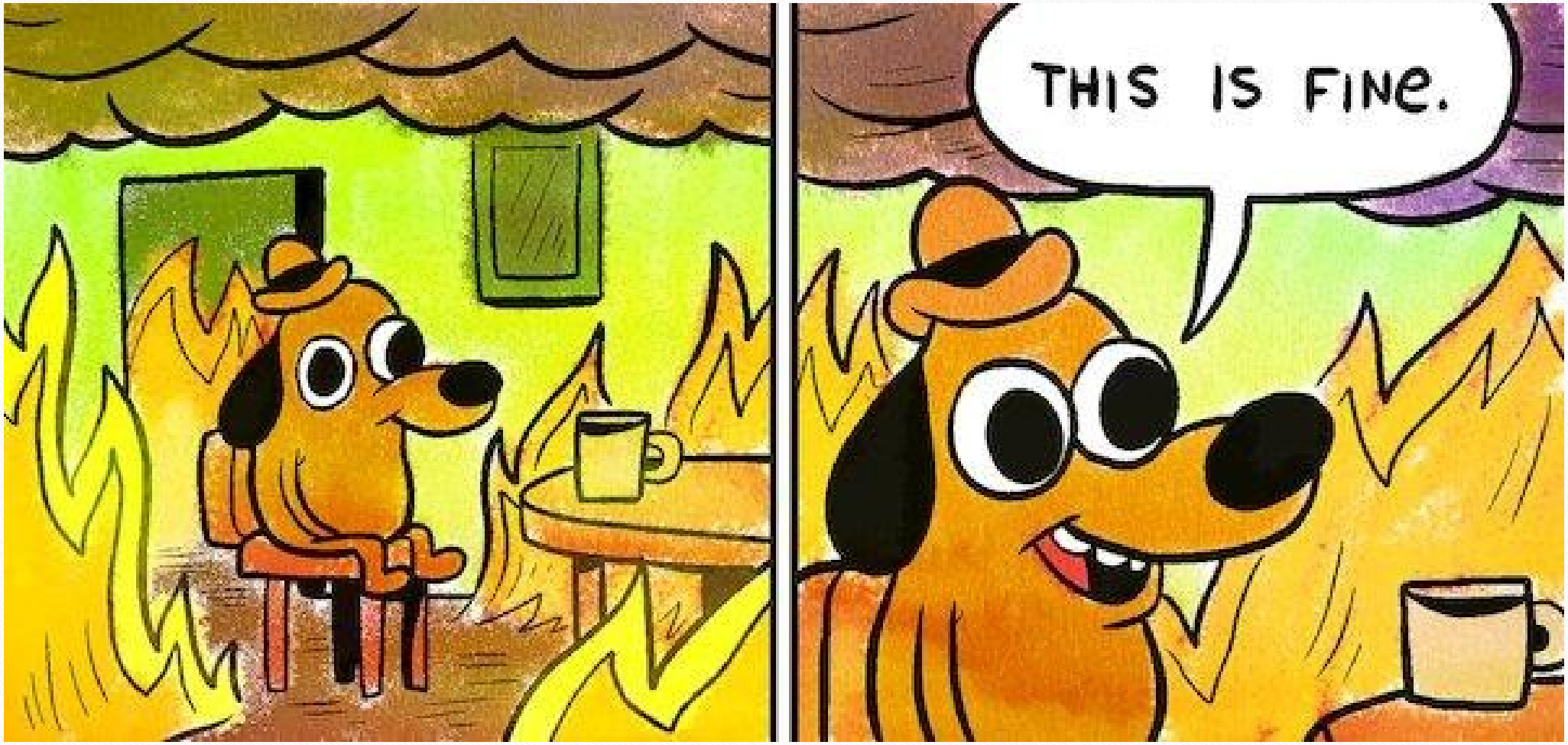
At Krones AG, a 15,000-employee German producer of bottling equipment, almost 60 people are involved in GDPR preparations. "The bigger an

https://www.bloomberg.com/news/articles/2018-03-22/it-ll-cost-billions-for-companies-to-comply-with-europe-s-new-data-law

¯_(ツ)_/¯

The GDPR requires the regulator to do something to enforce the law. It might not be a 4 percent fine, but they can't just forward the complaints straight to the wastebasket. "If they get hit with 10,000 complaints in the first month, they're going to be in trouble," says Straight. Seventeen of 24 European regulators surveyed by *Reuters* earlier this month said they weren't ready for the new law to come into effect because they didn't yet have the funding or the legal powers to fulfill their duties.

https://www.theverge.com/2018/5/22/17378688/gdpr-general-data-protection-regulation-eu


THIS IS FINE.

After May 25

- Lots of complaints submitted…
- But no enforcement to date
-

GDPR 101

“GDPR”

- General
- Data
- Protection
- Regulation

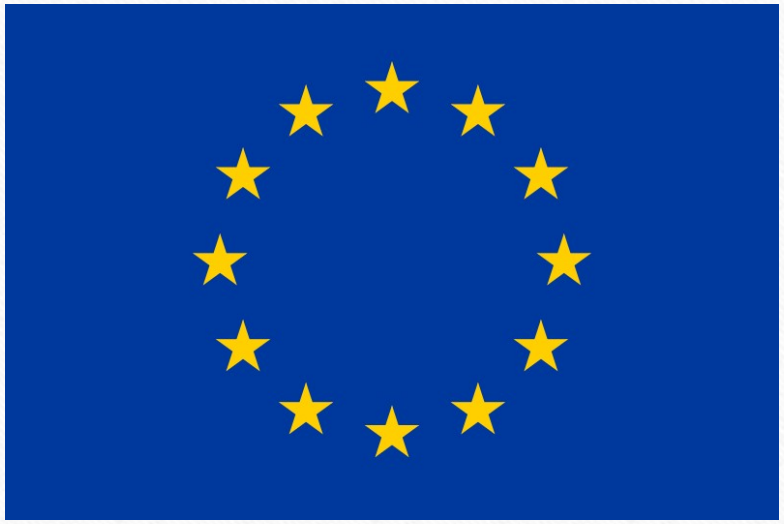
https://gdpr-info.eu/

Core Principles

- Have a really good reason to use other people’s personal data
- Don’t be sneaky
- Be careful with the information you have
- Personal control of data

Who It Covers

- Everyone who gets **personal** data from European Union residents



What Is “Personal Data”?

- Any data that can individually or collectively identify a “natural person,” including:
  - Name
  - Email
  - IP address
  - Combination of information, e.g., member of OSMF Board & lives in Switzerland…
-

What Activities It Covers

- “Processing”
- Storage
- Transfer

Exemptions

- Personal & household activities
- Government/public safety

Acceptable Reasons

- “Legitimate interests”
- Express & freely given consent
- Performance of a contract
- Others less relevant to OSM…

Extra Restrictions on Special Categories

- Information about minors (younger than 16 years of age)
- Sensitive information (religion, political affiliation, health information)

Disclosure Requirements

- Must publicly disclose:
  - types of data collected
  - purposes of collection
  - length of storage
  - data transfers
-

“Right to be Forgotten”

- Relevant if personal data is stored/processed on the basis of consent
  - when that consent is withdrawn, and there is no other lawful basis, data must be deleted
- Not required if processing in on other lawful basis – must evaluate need in light of deletion request

Data Transfer

- All international transfers must comply
- Acceptable circumstances:
  - Transfer to an EU member nation or an approved jurisdiction.
  - Standard contractual clauses
  - Performance of contract
  - Express consent

OSMF Preparations

OSMF Concerns

- How does GDPR fit with OSM’s purpose and activities?
- Personal data on the map
- Metadata containing personal data (usernames/userids)
- Personal data stored by OSMF (membership info, IP addresses)
- Other personal data volunteered by mappers (profiles, diary posts, etc)
-
-
-

OSMF Timeline So Far...

- Aug 2017 – Working Groups and Board start thinking about potential impact of GDPR on OSM and begin information gathering
- Sept 2017 - LWG gets helpful (free) feedback from law firm; LWG reaches out to WMF for advice
- Oct-Nov 2017 – LWG begins preparing white paper laying out situation and impacts
- Jan-Feb 2018 – LWG considers options and prepares recommendations
- Mar 2018 - LWG researches option re mappers who are minors
- April 2018 – LWG gets (free) feedback from lawyer connected through Brussels Privacy Hub on plan and recommendations. The white paper is published and discussed by the community.
- May 2018 – Board publishes blog post about preparations; LWG drafts new Privacy Policy based on recommendations
- June 2018 – New Privacy Policy released. LWG drafts new Terms of Use based on recommendations
- July 2018 – LWG drafts new NDA for OSMF volunteers

OSMF Conclusions

- Everything must have a justification!
- Much better for OSMF to rely on legitimate basis instead of consent – fits better with OSMF's purpose, goals, and practices
- We need to tighten up some data practices to fit with GDPR
- 24 page long draft whitepaper from LWG - https://wiki.openstreetmap.org/w/images/8/88/GDPR_Position_Paper.pdf

OSMF Changes

- Privacy Policy
- Terms of Use
- Access to personal data controls
- Internal access limitations
- Required disclosures
-

Privacy Policy

- Published
- Detailed description of data OSMF collects and what it is used for
  - Almost all of this was previously disclosed, but not in an organized fashion
  - Explanation of how long different types of data is kept

New Terms of Use

- Draft available, feedback welcome
- Explicit limits on use of personal data in OSM
- Codifies previous limits that were not expressly stated or were less visible, e.g.:
  - No spam or API/infrastructure abuse
  - No IP infringement
  - Limit OSMF’s liability

OSM’s Legitimate Interests

- Supporting OSM’s overarching goal of an accurate open worldwide map
- Map integrity
  - Validation
  - Investigation/correction of copyright, privacy, other issues
  - Detecting/blocking spam or vandalism
- Communication and feedback about map data, mapping techniques, and supporting infrastructure and tools

New Personal Data Limitations

- Use limited to those to have agreed to the Terms of Use (usually as evidenced by logging in)
  - API – some fields will require login to access, e.g., username, userid
  - Two versions of planet files – with and without username/userid
- OSMF storing IP addresses for a shorter time & masking
- OSMF formalizing limitations on access to membership data & systems data
-

Not Changing

- Your email is still generally private
  - Admins will still have access
  - Private messages will still be routed to you
  - You can voluntarily disclose it by sending an email on the forum or otherwise communicating it
- IP address still limited to admins
- Sharing your real name in your username, diary, wiki, talk-list, etc. completely voluntary (unless you’re a minor)
-

GDPR for OSM Community Projects

- If you passively use OSM map data
  - For disclosing information to your users about OSM, see https://wiki.osmfoundation.org/wiki/Services_and_tile_users_privacy_FAQ
- If you run an editing tool
  - You and your tools' users have legitimate interests in knowing info like usernames, but you should not go beyond uses covered by legitimate interests
  - Both agree to the Terms of Use (easiest way is to have users login with their OSM login)
  - Provide information to OSMF describing you and your use, so that OSMF can list in a common disclosures page

Example: OSMCha

- Ingests & allows users to manipulate data fields that are likely to contain personal data
  - E.g., username, userid, changesets
- Legitimate basis:
  - Catching bad edits, vandalism, spam
- Require a login
  - In progress
- Disclosures: Forthcoming

Example: hdyc

- Ingests & allows users to manipulate data fields that are likely to contain personal data
  - E.g., username, changesets
- Legitimate basis:
  - Research editing patterns, connect with nearby mappers for support & synergy
- Requires a login
  - Completed pre GDPR
- Disclosures: Forthcoming

GDPR for OSM Research

- Processing for research purposes is compatible for legitimate interests
- Document your research purpose and why you need the personal data
- Contact OSMF if you require access not available through regular Terms of Use
- Do not further share personal data without special agreement (summaries of your research that do not contain personal data should be okay)

Obligations of a “Controller”

- Inform data subjects of their rights
- Notification obligations in case of data breach
- Don’t process/store/transfer personal data without lawful basis
- (Document your storage/processing and lawful basis)
-

What’s Next?

- Community discussion of proposed Terms of Use and Board vote
- Technical implementation
- Communications to all users

Open Items

- Template for informing OSMF of your project’s use
- OSMF page disclosing list of projects using personal data from OSMF
- Way to propagate list of deleted userids to projects

FAQs

Does this affect my use of an OSM map?

- Probably not
- If you are using OSM to navigate the world (viewing some form of maps and/or searching points of interest information, and routing instructions), that information should not be affected because it’s not using personal data.
- OSM data is still under ODbL.
-

How does this change how I edit the map?

- Your contributions will not change.
- Access to some metadata useful for editing, like username/userid, will be limited to users who have agreed to the new Terms of Use.
- Your favorite editor may update to accommodate.
-

What metadata will require agreement to ToU?

- Usernames/userids
- Edit history information (# of changesets, blocks, traces, etc.)
- Comments/notes
- Changeset id
- Timestamp? (may be partially obscured)

What about my project? It uses X!

- **If you use affected metadata, GDPR applies to you and your users.**
- May need to take compliance measures, for example require users to log in to their OSM accounts, demonstrating that they have agreed to ToU.
- LWG is working on providing templates and more information.
-

Questions?

legal-questions@osmfoundation.org

Further Reading

- Blog post from OSMF Board “Preparing for the GDPR” https://blog.openstreetmap.org/2018/05/14/preparing-for-the-gdpr/
- Heather Leson’s diary post “GDPR Primer for OSMF” https://www.openstreetmap.org/user/Heather%20Leson/diary/43785
- Text of GDPR https://gdpr-info.eu/
- LWG GDPR whitepaper https://wiki.openstreetmap.org/w/images/8/88/GDPR_Position_Paper.pdf
- Privacy Policy https://wiki.osmfoundation.org/wiki/Privacy_Policy