Open Social

GDPR

Version	Date
1.0	**May 2018**

Index

Disclaimer: this article should not be used as legal advice for organizations when it comes to the compliance of data privacy laws such as the GDPR or USA regulations. It is background information to inform readers about the GDPR, U.S. data privacy laws, and how Open Social has ensured its own compliance.

The USA and the EU have a fundamentally different approach to privacy and data laws. This article provides an overview of EU laws such as the GDPR, USA data regulations, and how the data of both EU citizens and USA citizens are protected by Open Social.

The EU and the U.S.

The present and the future of the internet are fueled by data. In some areas of the world, data regulations are becoming stricter. In others, the rules that govern the use and collection of private data are not so clear yet. **Our EU and USA customers benefit from the various security and privacy regulations implemented by Open Social.**

The EU views privacy as a human right and has implemented laws and regulations with that philosophy in mind, even before the upcoming GDPR. There is one general law that covers the collection of personal data of EU citizens, which ensures that nothing can happen to this data without the consent of the individual subject. Open Social is placed under EU legislation and we follow strict data and privacy laws and regulations. We are currently working hard to adhere to the new regulations outlined by the upcoming GDPR.

The USA, on the other hand, does not have the same approach to privacy. This is partially due to the history and commitment to the first amendment: the right to free speech. Instead, privacy laws are created when there is a need for them. The regulation of private data also depends on the category that the information belongs to. For example, health data is regulated by the HIPAA, the marketing data by the TCPA, and so on (read more about this below).

What is the GDPR and how are we ensuring compliance? Which data privacy laws and regulations exist in the USA? How does this compare to the EU? How are you protected as an Open Social customer? Continue reading to find out!

GDPR and EU Privacy Laws

Introducing the GDPR

The GDPR is an EU legislation that became operative on the 25th May 2018. It enhances the protection of the personal and private data of EU citizens and ensures that organizations comply with various obligations when they collect and process personal data. It replaces and builds upon the 1995 EU Data Protection Directive (DPD) and its terms on data privacy and security but includes a few new additions that focus on the rights for secure personal data and stricter penalties for noncompliance. Moreover, the GDPR is a directive that will 'harmonise' data privacy laws across Europe. It applies to the 27 member states at all levels of the law; local courts, supreme courts, and eventually the EU Court of Justice.

Why is did this come into effect? The amount of digital information collected and stored has vastly increased since its creation in the '90s. Since then, a need for stricter data regulation and privacy has become necessary to protect the information of web users.

It's important to note that even if your organization is based outside the EU, the GDPR is still applicable if you are processing the data of EU citizens.

What is it?	EU legislation that serves to enhance the protection of the personal data of EU citizens.
When will it be enforced?	May 25, 2018
What is new?	People have new rights regarding the information that companies have about them, companies are obligated to have better data management, and there are stricter fines.
Who does it apply to?	Any company controlling or processing the data of EU citizens.

Figure 1. GDPR Summary.

What is needed to comply?

The GDPR document consists of 99 articles dedicated to the rights of individuals and the obligations for companies to comply with the new legislation. Many of the principles outlined in the GDPR are the same as those in the DPD and the Data Protection Act (DPA). So, if an organization already complies with the current data protection laws, then they will already be complying with many of the GDPR principles. Below you will find an overview of the most important components of the GDPR (please be aware that this is not comprehensive and does not replace the legislation).

- **Access and portability.** You must allow the customer to access their own data and transfer it to another organization if requested. This is the right to data portability. This is new in comparison with the DPD and DPA and is one of the most challenging aspects of the GDPR.

- **Erase data.** Customers have the right to demand that their data is deleted or object to the way it is processed, as long as it does not interfere with freedom of expression or the ability to research. The controller also has the responsibility of telling other organizations (such as Google) to delete any copies of the data as well. This is the right to be forgotten and is new in comparison with the DPA and DPD.
- **Check if you need a data protection officer.** You must have a data protection officer if you collect data on a large scale or deal with sensitive data. Read more.
- **Clear communication.** You must inform customers/visitors who you are when you ask for their data. You must also explain why you are processing their data, how long it will be stored for, and who will receive it.
- **Consent.** You must get clear consent for collecting data. If you're collecting data from children, you must check the age limit for parental consent.
- Warnings. You must inform the customer of serious data breaches within 72 hours of learning about it.
- **Profiling.** If you are using data for profiling and processing applications for legally-binding documents then you must inform your customers, have a person (not a machine) checking the process, and offer the customer the right to contest a refusal. Open Social does not use any form of profiling.
- **Marketing.** You must give people the right to opt-out of direct marketing that uses customer data.
- **Sensitive data.** You must use extra safeguards on information such as race, health, sexual orientation, religion, and political beliefs. For most projects that means at least encrypting the stored data.
- **Data protection by design.** You should build data protection safeguards into your product and services in the early development stages. This is the requirement to build in data privacy by design.
- **New technologies.** You are obligated to conduct a Data Privacy Impact Assessment (DPIA) when you process new technologies.
- **One-stop shop.** If you have offices in multiple EU countries, then you must have a lead supervisory authority for a central point of enforcement.
- **Keep records.** You must keep data records if you process data regularly, collect sensitive information, and if the data you collect is a threat to people's rights and freedom.
- **Data transfer outside the EU.** You must make extra arrangements when transferring data to countries that have not been approved by EU authorities.

There have been many checklists surfacing online in order to help companies comply. For example, The Office of the Data Protection Commissioner created a great GDPR checklist.

The local Data Protection Authority will be monitoring the compliance of organizations, which is coordinated at an EU-level. The cost of noncompliance is high. It will result in warnings, reprimands, suspension of data processing, and fines as high as €20 million or up to 4% of global annual turnover. In other words, organizations can't afford to ignore the legislation and it should be everyone's priority to ensure compliance.

U.S. Data Regulations and Laws

A patchwork of data privacy laws

There is no single, comprehensive law regulating the use and collection of personal data in the USA. It's best described as a patchwork system, where various federal and state laws overlap and even sometimes contradict one another. Under the state and federal laws, there are many self-regulatory guidelines developed by industry-specific groups and governmental agencies. Although these are not enforced by law, they are considered 'best practices'.

For example, the advertising industry has developed a program to self-regulate online behavioral advertising. It ensures that members of various advertising industry trade groups comply with the guidelines.

Federal privacy laws

There are various federal laws that regulate the collection and use of private data. Some of them apply to categories of information (such as financial or health) and others to the use of personal information by e-commerce and telemarketing. Moreover, there are various consumer protection laws that aren't specific to privacy and data but prevent deceptive practices that involve the sharing of personal data.

However, most of the primary health and security privacy laws only apply to "covered entities" that are holding "protected health information", meaning that vague terms are used in the laws. Moreover, federal regulators acknowledge that most of the American people do

not know when their information is protected by the law or not and when security standards apply.

Some of the most important federal privacy laws are:

- The Federal Trade Commission Act (FTC). This is a consumer protection law that prohibits unfair and deceptive practices in privacy and data security.
- The Financial Services Modernization Act (GLB). This act regulates the use, collection, and disclosure of financial information by financial institutions (such as banks, insurance companies, etc.) and organizations that provide financial products and services.
- The Health Insurance Portability and Accountability Act (HIPAA). This act is responsible for regulating medical information and applies broadly to health care providers, pharmacies, and any other organization that handles medical information.
- The Fair Credit Reporting Act. This law regulates the sharing and collection of consumers reports by consumer-reporting agencies (such as credit card companies).
- The Electronic Communications Privacy Act and the Computer Fraud and Abuse Act. These acts regulate the interception of computer tampering and electronic communications.

There are other various regulations. Find them here.

State privacy laws

There are laws at a state level that regulate both the use and collection of personal data, and we are happy to see that the number of laws keeps growing. However, these laws often have very different and incompatible regulations about the type of personal information that requires protection (such as the notification security breach law), and what even constitutes as a breach of privacy. In general, most states already have a form of data privacy regulation, with California clearly taking the lead.

California has implemented various laws surrounding privacy that have had nation-wide effects. Their security breach notification law, which forces anyone that owns computerized data to inform users of data security breaches, inspired the whole country to implement the same. Recently, as of March 28, all States now require notifying customers of any security breaches of their personal data.

GDPR vs U.S. Data Laws

The GDPR is introducing strict regulations to the way personal data is handled by organizations. The USA has yet to catch up with stricter data regulations. Here is how the GDPR compares to existing USA data laws.

Does the USA ensure that data controllers process data properly?
There are only a few laws that regulate organizations and the way they process personal data. Although the FTC does not require organizations to have a privacy policy, it both ensures and charges those that do not comply with their own privacy policies when they have one. The GLB Act protects consumer privacy by restricting when personal information can be disclosed, and organizations must notify users when their disclosing the information and offer an option to opt-out.

Are users asked for consent before processing personal data? (Consent)
Although there are laws that ensure that users are asked for consent, it only really applies to sensitive personal data such as health, financial and social security information. The FTC suggests that website operators should get confirmed consent before using sensitive personal data. The GLB Act requires that financial institutions should at least confirm consent annually. Also, HIPAA requires medical institutions to obtain written consent before sharing medical data.

Are there any specific rights for data subjects? (Data Access and Portability)
Most USA privacy laws generally do not provide data subjects with specific access rights to their own data. The FTC requires organizations to share their privacy procedure, at the least, and inform users how they can opt-out of data sharing if they want to. The HIPAA requires medical institutions to share how consumers can access their information.

Are data subjects able to delete their data? (The right to be forgotten)
In the USA, data subjects currently have no rights when it comes to the deletion of their data under federal law. The closest that comes to this law is HIPAA, which allows users to amend inaccurate or incomplete information (although the organization is not complied to actually adopt the suggested changes).

Privacy Measures for Open Social

GDPR Features and Roadmap

Open Social has a user-centered design, in which user freedom of choice, privacy, and security are at the forefront of our design choices. This means we are naturally compliant with most of the GDPR.

In terms of GDPR-compliance, there are a few fundamental actors. These are defined for Open Social as follows:

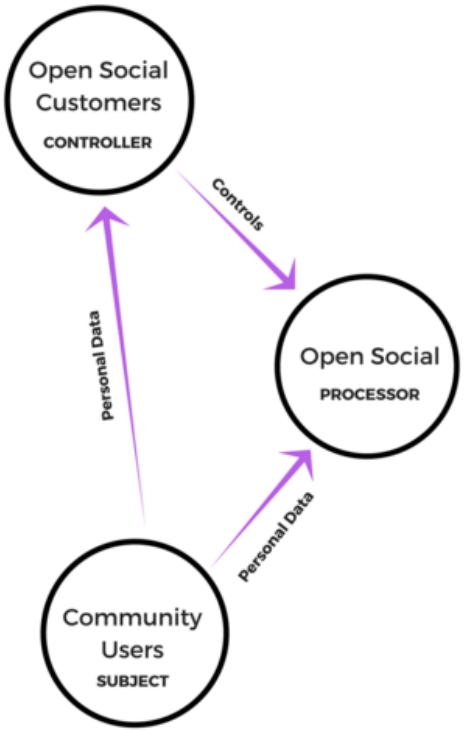

Figure 2. GDPR Data Triangle.

- **The Data Controller:** Open Social customers. This is the entity that decides the means, purpose, and processing of the data.
- **The Data Processor:** Open Social. This is the entity that handles and processes the personal data on behalf of the controller.
- **The Data Subject:** Users of an Open Social online community. This is who the law has been designed to protect.

In order to ensure full compliance, Open Social reviewed its external and internal processes. We found that we needed to work on the following:

- Improve communication about what happens with our user's data.
- Provide site managers with the ability to minimize the collection of personal data.
- Encrypt personal data by default.
- Allow users to export their data from Open Social.
- Assign a Data Protection Officer (DPO).
- Scope our security controls using a framework.

Privacy by Design

We have already begun working on becoming GDPR compliant and adopting the Open Social product to the points above. *Open Social has implemented the following features to ensure both our own and our customers' compliance with the GDPR regulations*:

Ask for consent to data policies

This feature allows site managers to create and update the data policy of their community, and allow regular users to either provide or withdraw consent to each revision of the data policy. The consent to the data policy can be made mandatory or optional.

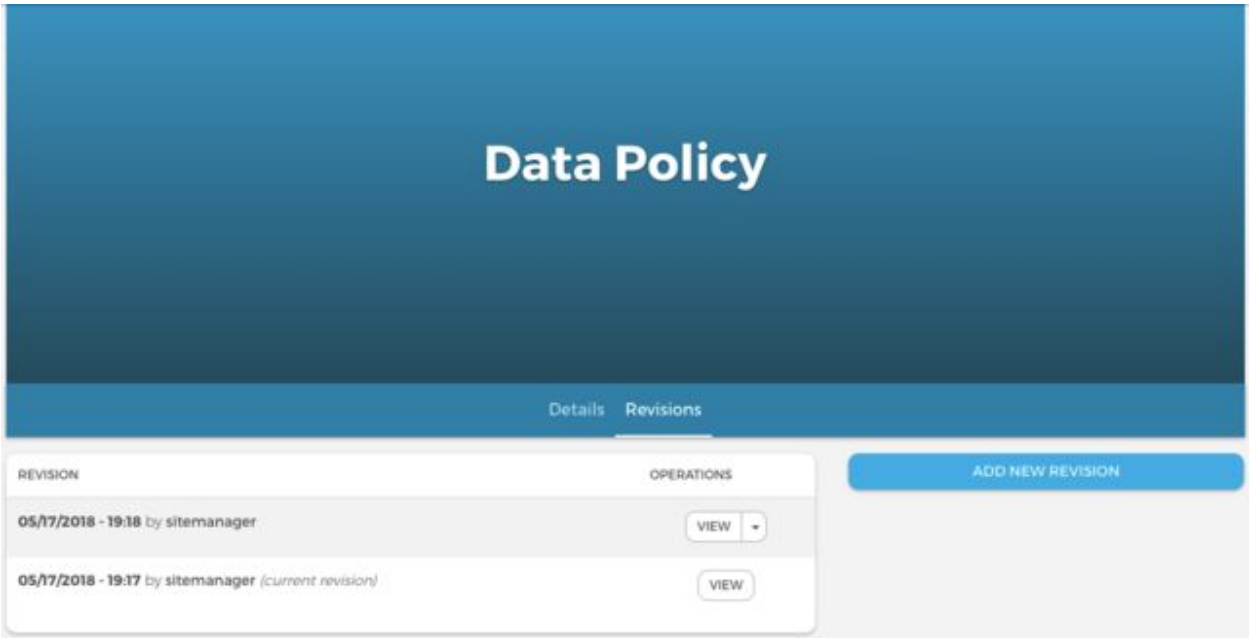

Figure 3. Site managers can create and update data policies.

Regular users can give or withdraw consent to each active revision of the data policy.

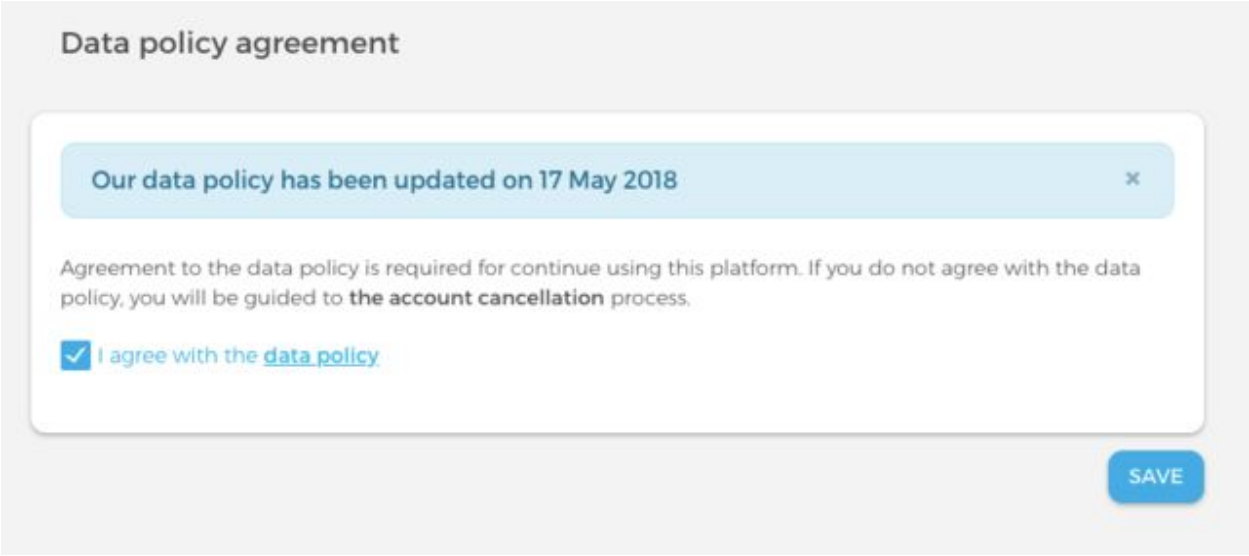

Figure 4. Data policy in Open Social.

Inform users of data usage

In an online community, there are a few pages where personal data is collected (sign up page, settings page, and edit profile page). Site managers add a block to these pages to explain to users which data will be collected and why it's needed.

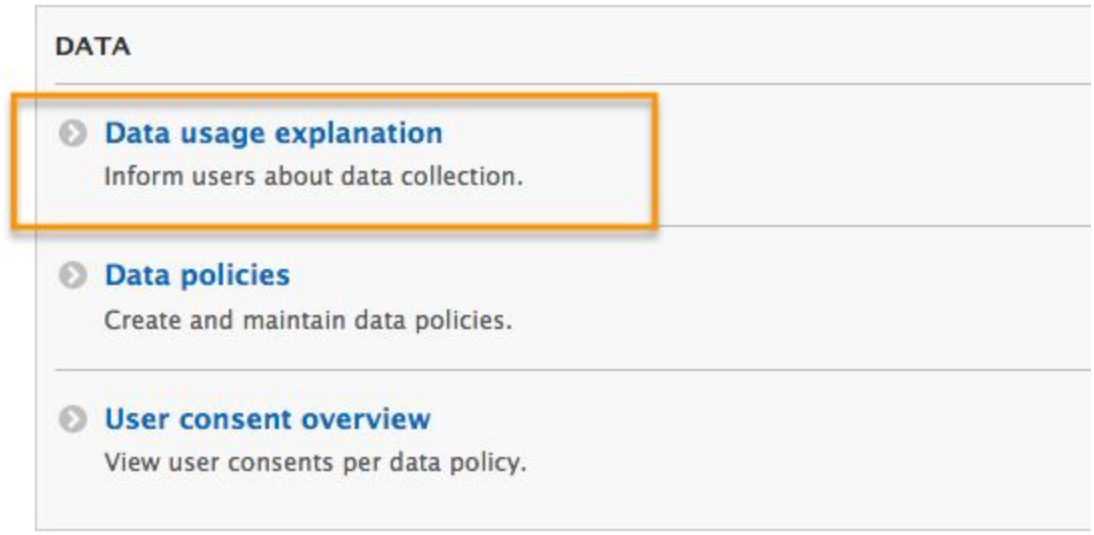

Figure 5. Explain to users which data will be collected and why it's needed.

Disable profile fields

We wanted to limit the amount of personal data that's collected within a community. Therefore, site managers can choose to disable certain profile fields on profile pages. Moreover, users themselves can decide which profile fields they would like to display on their own profile page.

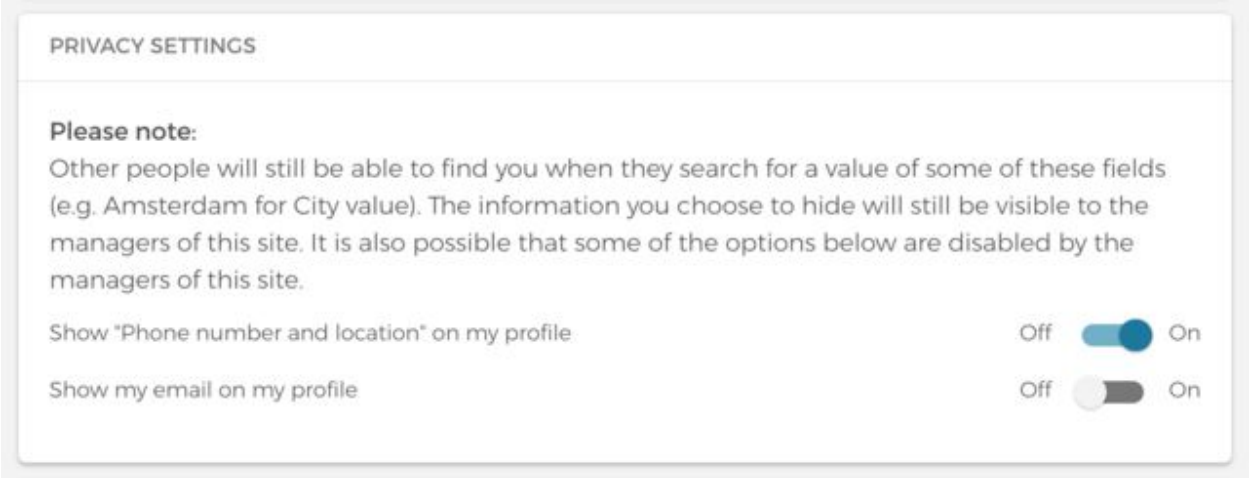

Figure 6. Users can choose which data fields to display on their profile.

Delete a user account and remove personal data

Open Social users have always had the right to delete their account in Open Social. This process has been improved for the GDPR. Users can delete their account, their profile information, and their private messages. Any other content that they created will be anonymized. The community users will also be clearly informed about what will happen to their personal data after the account has been deleted.

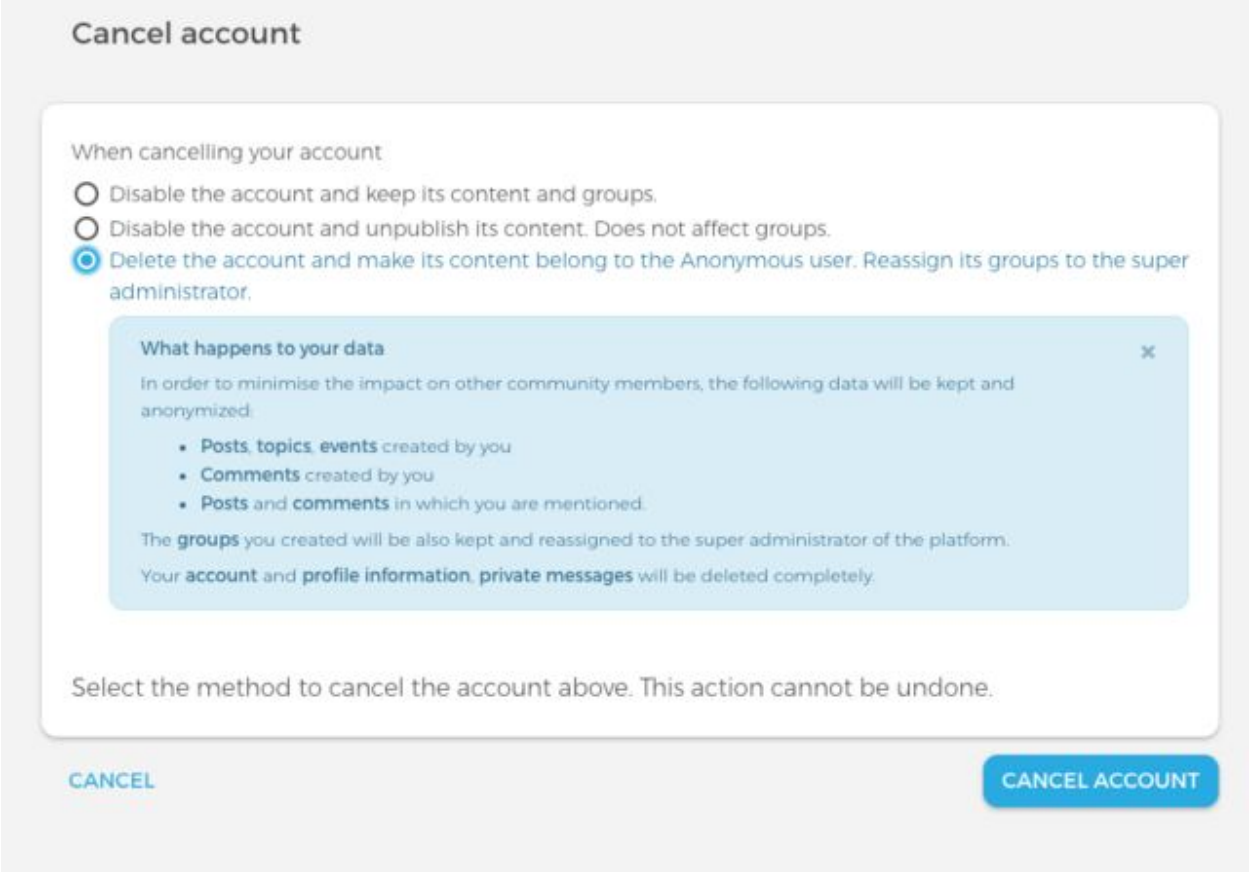

Figure 7. Users can anonymize or un-publish their content and delete their account from our community platform.

Content Visibility

When a user adds any type of content to the platform such as a blog or timeline post, users can choose the visibility of the content: public, community only, or just for group members.

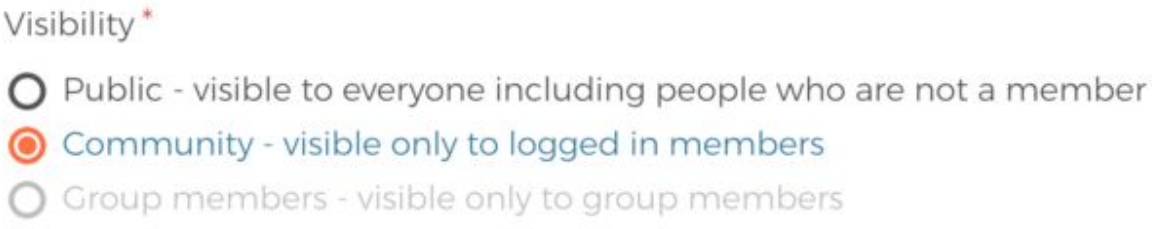

Figure 8. users can choose the visibility of their content.

We are also documenting our processes, which provides a stronger understanding and overview of our data management strategies. To stress the importance of privacy, we appointed our co-Founder Taco Potze as Data Protection Officer. Our end goal is to ensure that one, Open Social complies with the GDPR and two, that the data controllers (our customers) have the tools to comply with the GDPR as well.

See all our GDPR features here.

Why is this important?

Many organizations may need to adapt their security and marketing handbooks, but we have a good head start on the GDPR and a good understanding of USA regulations and laws. We also recognize that the new regulations have various benefits for both customers and organizations. Here are the top ones:

- **More transparency between organizations and end-users.** Once all organizations comply with the GDPR, EU citizens will have a lot more control and transparency in how their data is used.
- **Greater value for organizations and end-users.** In the long term, the access and portability component of GDPR will increase the value of services that are allowed to process the data of their end-users. This will only come into effect when it has been defined legally by the courts and has been implemented by all major software solutions.

Both our USA and EU customers will be notified of any changes that will be made to the functionality or regular use of Open Social. This page will also be updated over the coming months, so feel free to return at any time!

Further Reading

- The full GDPR regulation
- The EU GDPR official website for regulation
- Open Social Security Overview
- Data Protection in the United States

Next: EU ePrivacy Regulation

Although the GDPR is gaining a lot of attention, new EU legislation is already on the horizon and is expected to go into effect in 2019. It's currently called 'Directive on Privacy and Electronic Communications' (Directive 2002/58/EC and the 2009 update, Directive 2009/136). The newcomer is the ePrivacy Regulation and aims to update the EU's ePrivacy legal framework. The new regulation will complement the GDPR and similarly strives for regulation uniformity across the EU. As online privacy and security is a topic that needs continuous effort, we will keep Open Social in line with applicable laws wherever we can. Read more about the ePrivacy Regulation.