Five tips to ensure your project is GDPR compliant

Consulting experts and the public and incorporating their feedback into your project is a fundamental aspect of Human Practices. It's informative and fun, but simultaneously imposes responsibilities on your team. Especially since May 2018 the General Data Protection Regulation (GDPR) is enforced by the European Union (EU), which has a global effect. The law gives EU citizens more control over their data. The rules can be quite overwhelming, so in this article we point out five important highlights for your team to take into account and getting you started.

Interviews and surveys are a very effective way to gain invaluable insights for improving the impact of the project. Information from such consultations may be personal data. This is where the GDPR comes into play. The law has specified instructions on how you should handle the data resulting from interactions with residents of the EU, even when you are located outside of the EU.

Data which is deemed personal can be basic identity information, such as mentioning a name on your wiki. Email addresses, locations, genetic data and political opinions are also examples of personal data. Basically any information that may be traced back to a specific person is personal.

Serious violations of the GDPR may lead to penalties up to 20 million euro or 4% of annual turnover of your institute, whichever is higher. Anyhow complying to the GDPR is a matter of respecting an individual's privacy. Here are five tips to get your GDPR compliancy started:

1. Ask for consent

Whenever you collect personal data, you need to make sure the subject provides you with consent to manage their data. It is your responsibility to inform the subject about the purpose of the data collection, where you store it, for how long and in which ways you may use it in the future. You may not use the data outside the scope of the consent. Consent forms or asking for consent in an email are an effective way to deal with this obligation.

2. Provide an opt-out option

The GDPR insists that you respect the right to be forgotten, also known as data erasure. EU residents have the right to have their data deleted and stop processing by a third party entirely at any time. Make sure you inform the subject upfront about whom to contact in order to have their data removed.

3. Store personal data safely

As a personal data collector it is your responsibility to store data safely. Technical measures must be in place to manage access to documents such as attendees lists of an event, transcripts of an interview or contact details of sponsors. A practical way of complying is adding an extra layer of protection to your files, especially in case the files are stored on a shared network drive like Dropbox or distributed via email. Most spreadsheet programs have an option for password protection. Otherwise storing files in password protected ZIP archives as another convenient approach.

4. Respect the individual rights to their data

EU residents have the right to obtain confirmation about whether their data is being collected, processed, and if so where it is being processed and for what purposes. You must reply to these request free of charge. Moreover, you must facilitate data portability, meaning that the subject may request a copy of all their personal data you may have in your possession.

5. Set up a notification system in case of a data breach

In case the data gets stolen by hackers, accessed unauthorized in any other way or processed beyond the scope of the consent, you have to notify the subjects and the Information Commissioners Office (ICO) of your institution within 72 hours. Make sure you have set up a procedure to do so in advance, the timeframe does not leave a lot of room for improvisation.

These five tips ensure you have covered the most important aspects of the GDPR. Implementations of the regulation may be country or institution specific. Be sure to check with the ICO or similar department in your institution for full compliance. By doing so you live up to the standards of responsible research both inside and outside of the lab.