Exercise 1 - Privacy and Data Protection

1. Valid Consent?

For this research I've chosen the website medium.com, a very famous american online publishing platform. The privacy policies can be found at this link: https://help.medium.com/hc/en-us/articles/360052305234. As the reader could see, the policy is composed by three sections: **Medium Privacy Policy** (general privacy policy), **Data Protection Statement for European Union Users** (with reference to the GDPR) and **Consumer Privacy for California Users** (with reference to the CCPA, California Consumer Privacy Act); I will focus on the second section, the **Data Protection Statement for European Union Users**, since it's the current law in our case [`Art 3 (1) GDPR` and `Art 3 (2) b) GDPR`]. I will now analyze the important parts of thje privacy policy step-by-step.

Lawfulness of processing

First of all, this privacy policy agrees with the Lawfulness of processing, since it fulfills at least one of the point in [`Art 6 (1) GDPR`]; to be more specific, it fulfills: [`Art 6 (1) a) GDPR`], since the website asks for consent to process personal data for (many) specific purposes, which are reported below.

Purposes of processing

The privacy policy states that the purposes of data processing are the following (verbatim):

- *Provide, test, promote, and improve the Services*
- *Gather usage statistics of services*
- *Provide customized reading experience*
- *Publish and distribute user-generated content*
- *Provide access to paid content*
- *Pay authors in Partnership Program for certain content*
- *Fight spam, fraud, and other abuse of services*

These points are in agreement with [`Art 5 (2) GDPR`].

Categories of Personal Data Collected

The website distinguishes between logged out and logged in users; it collects the following data from logged out users:

- *Reading history*
- *IP address*
- *Browser information*
- *DNT status*

And the following form logged it ones:

- *Username*
- *Display name*
- *Bio*
- *Avatar image*
- *Email address (non-public)*
- *Session activity (security)*
- *Linked social media accounts (optional)*
- *IP address*
- *Browser information*
- *Reading history (on Medium Services only)*
- *Meta-data about URLs saved by using the optional feature Save to Medium*
- *Network interactions (recommends, follows, etc.)*
- *Posts, responses, or series published by user*

Both the logged out and logged in user data is sensible data, in accordance with the GDPR; nevertheless, as stated previously, lawfulness of processing subsists, then this part is in according with the law.

Use of Algorithms to Personalize User Experience

The policy states that (verbatim):

Medium collects and stores personal data about its users to customize their reading experience by displaying content tailored to the preferences and interests indicated by the users (including through their reading history and Services interactions). This does not constitute automated decision-making as that phrase is used in the GDPR because it does not produce any legal effects or similarly significant effects for users. Medium also moderates content for the purposes of fighting and preventing spam, fraud, and other forms of abuse, and may rely on algorithms as part of doing so.

This part is in accordance with the GDPR, as stated by [`Art 22 (1) GDPR`].

Cross-border Transfers

The policy states that *"Medium is hosted in the United States. By using the Services, you authorize Medium to transfer, store, and use your information in the United States and any other country where we operate. Where your data is disclosed to our processors, it is subject by contract to at least the same level of data protection as that set out in this statement"*, and this is in accordance with the current law, which states that the geographical location of data storage is irrelevant from the moment the user is situated in the EU, [`Art 3 GDPR`].

Right of data subjects

The policy states that the rights of data subjects are the following (verbatim):

1. *If you sign up for a Medium account, you may at any time request an export of your personal information from the Settings page.*

2. *You may correct information associated with your account from the Settings page, and the Customize Your Interests page to update your interests.*
3. *You may withdraw consent by deleting your account at any time through the Settings page, which will erase your personal information completely within 14 days (except to the extent Medium is prevented by law from deleting your information).*
4. *You may object at any time to the use of your personal data by contacting privacy@medium.com. If your complaint relates to alleged misuse of your personal data by a third party, it may result in suspension of that post or account in keeping with relevant law, public interest, our contractual obligations, and the rights of expression and access to information of others.*
5. *Under EU law you have the right to lodge a complaint regarding the processing of your personal data by Medium with the dedicated Supervisory Authority of your EU member state.*

These five points satisfy and fulfill [`Art 13 GDPR` and `Art 15 GDPR`].

Conclusions

From a non-specialist opinion, Medium's privacy policy is in line with the current GDPR. Despite this, I focused on the "most famous" parts of the GDPR, which are also reported in Lecture 9 slides; I think that a more in-depth study should then be done by an expert, in order to assert that everything is according to law.

2. Your Right to Access your Personal Data

Rights to access your personal data

The right to access and manage the personal subject data is regulated by the following articles and sections of the GDPR: - `Art 15 GDPR`: right of access by data subject. These four articles talks the rights of the data subject to access its own data and the modalities to do so; - `Art 16 GDPR`: right of rectification, the right to rectificate wrong data; - `Art 17 GDPR`: right to erasure, the right to be forgotten; - `Art 18 GDPR`: right to restriction of processing, the right to restrict data processing and usage; - `Art 20 GDPR`: right to data portability, the right to change data location - `Art 21 GDPR`: right to object, the right to oppose to data usage.

Right to access request

I filed a request of right to access to my Medium account data. This website is not only GDPR-compliant, but it also offers easy-to-use tools to get personal data: in fact, it was enough for me to click on "Download your information" and wait for the email with my personal data stored in an accessible format (a `.zip` file containing many `.html` reports). In conclusion this, in addition to what I said in the first chapter of this document, leads me to think that my rights as data subject are respected.

3. Anonymisation & Pseudonymisation

At first sight, anonymisation and pseudonymisation seem to be the same procedure: it seems impossible, in fact, to infer real user data from both of them. There are, though, some key differences between them that make one out of the GDPR scope and the other in scope. Let's analyze them.

Anonymisation

We say that data is anonymous when the data subject can no longer be identified from it. This means that the anonymisation procedure must delete all the possibilities to recognize the subject.

Pseudonymisation

Pseudonym data is when the data itself is not sufficient to identify a subject, but adding further information can lead someone to recognize the original subject. Pseudonymisation is then the procedure of hiding personal data using a key; this key, for example a personal identification number, can be accessed only by authorized users.