1. Valid Consent?

In this set of question, I will choose to use the policy given by Google.

In Google’s Privacy Policy, data such as personal profile which we give out when registering and Geo-location, log information and device information when we give out because of using of their services will be collected.(Art4) So, their policy is in the scope of GDPR. Meanwhile, Google choose to let every user to consent with their privacy policy, which can be showed on the web page as well as any app published by Google.(Art6 1a, Art7 1) In this consent, Google list very specific purposes of why and how they are going to process personal.(Art6 1a) Also, except agree, there are other option given as the rejection of the data collection. And it can be revoked at any time.(Art7 3) In conclusion, as far as they have illustrated, I think their services are in line with new requirement.

2.Your Right to Access your Personal Data

I think my right is respect well in the privacy policy of Google. I am provided the access to most part of services. As I log in and get into the console of my account. I can customize my privacy setting and correct my personal data as what is requested in Article 16 and Article 21. GDPR also have regulation for the right to be forgetten(Art 17) , which is surprisingly is backed by deleting my account option. There are quite few website which will even mention it.

However, for some requirement of GDPR, I will not know if it is actively be in power. For example, Article 22 requires that data subject shall have the right not to be the subject to a decision based solely on automated processing, including profiling, which may lead to legal effect. In practice, we will never know whether we have been profiled. It seems that Google does not mention anything about decision-making things except for advertising. I can reject the data collection for advertising. Other than that, I just simply do not know if there is any.

3. Anonymisation & Pseudonymisation

Anonymisation is the way in which data will be processed in order to prevent the identification of the individual becoming known. Anonymisation will be considered effective if all methods that could be used to identify a subject fail. The Data Protection Act 1988 & 2003 (“Data Protection Acts”) only govern the area of personal data. If personal data is effectively anonymised, it is no longer considered “personal data” and therefore will not be subject to the Data Protection Acts. If anonymisation of data fails and/or is not possible, then the data must be continued to be treated as personal data.

Pseudonymisation of data means replacing any identifying characteristics of data with a pseudonym, or, in other words, a value which does not allow the data subject to be directly identified. Pseudonymisation often gets confused with anonymisation; however the two must be seen as different techniques. Pseudonymisation is not considered a form of anonymisation but instead, the ODPC recommend that it should be considered a “security enhancing measure” in order to reduce “linkability in a dataset”.

Care must be given to the reuse of a pseudonym, as the reuse of a pseudonym increases the risk of linking one dataset to another and identifying an individual.