Queen Mary University of London
Centre for Commercial Law Studies
67-69 Lincoln's Inn Fields
London
WC2A 3JB

qLegal@qmul.ac.uk
www.qlegal.qmul.ac.uk

Client Reference Number: [Confidential]

17th December 2021

Privileged & Confidential

By email to: [Confidential]

Dear [Confidential]

Re: Your Appointment with qLegal on 25th November 2021

How we work

Thank you for attending your appointment with us and for using the services of qLegal at Queen Mary University of London. Although we cannot provide you with representation in any proceedings and do not hold ourselves out to be a firm of solicitors or patent attorneys, our advice is free, and we aim to provide the same high standard of service expected in the practice of law. Please note that the legal advice provided is in relation to the laws of England and Wales only. If you require advice outside of this jurisdiction, please contact us.

Case Summary

[Confidential] (the "**Company**") was founded in early 2021. The Company is currently in the process of developing a mobile Application (the "**App**") to support [Confidential] suffering with [Confidential]. The App will contain a [Confidential] and [Confidential] for users to input information to as well as [Confidential]. The App is being developed by a third party.

The App will be launched in early 2022 on the IOS App store and on Google Play later on next year. The App will be available to download in the UK only. There will be a free and a paid version with both being ad free but the paid version containing more features.

Currently the Company has a website which mentions the awards that the Company has won and a blog where users can submit their own stories relating to [Confidential] and [Confidential]. There is also a mailing list which users can sign up to and receive a monthly newsletter from the Company. The website is currently being hosted and run by [Confidential].

From a data protection perspective, we understand that:

- The Company will be collecting personal information from users.
- The information collected will be stored in the [Confidential] (for the website) and [Confidential] (for the App) servers, the servers may be located outside of the UK and EU.
- All information collected via both the App and website will be shared with third parties.
- The website is run and hosted by [Confidential].
- The App is being developed by a third-party App developer whom the Company currently has no written agreement with.

Scope of Advice

You have asked us to advise you on the following:

1. How to comply with your data protection obligations.

2. To provide a template cookie and privacy policy.

Summary of Advice

The Company must comply with the UK General Data Protection Regulation ("**UK GDPR**"), the Data Protection Act 2018 ("**DPA 2018**") and the Privacy and Electronic (EC Directive) Regulations 2003 ("**PECR**") regarding the handling of personal data collected from users.

We have attached a document containing standard templates for the privacy policy and cookie policy conditions for your convenience. It is important to tailor these policies to suit the interests and practices of the Company.

It is strongly advised that the Company draws up a contract with the App developer if they are going to be processing any personal data on behalf of the Company, so that the Company complies with its data protection obligations.

Explanation

What is the UK GDPR?

The UK GDPR is a legal instrument that governs the collection and use of personal information from individuals in the UK. This framework has imposed obligations on those who collect and use this information and has granted rights to individuals whose data is being collected. Article ("**Art**") 5(1) UK GDPR sets out the key principles of data protection. It states that the data collected:

- Must be lawfully processed in a fair and transparent manner. In other words, the Company must have a lawful basis for processing the data that is collected. Consent is one such basis and if the data being processed is sensitive data, then explicit consent may be needed. However, consent is not the only basis, and the Company may process the data if it has a 'legitimate interest' in doing so, or if the

processing is necessary for the performance of the contract with the individual (among other reasons).

- Should be relevant and limited to what is required.
- Must be accurate and kept up to date.
- Must not be stored longer than necessary. Any data that is no longer required should be deleted.
- Must be protected against unauthorised use, loss, or damage.
- Must be used in accordance with its specified purpose and nothing more. This purpose must be specified in the privacy policy and could be, for example, to register an individual's account, or to notify them about changes to the Company's privacy policy.

What is Personal Data?

Personal data is any information relating to an identified or identifiable natural person ('data subject') (Art 4(1) UK GDPR).

We understand that each user will have to create an identification (ID) profile which requires disclosing personal information such as their name, contact details, gender, bank details, home/work address and so on. This kind of information falls under the category of personal information as they can be used to identify an individual. If the information collected cannot be used to identify a person and is therefore anonymised, it is no longer classified as personal data. Hence, the UK GDPR and other data protection laws will not apply.

Special Categories of Personal Data

The Company collects '[Confidential]' from users, which inevitably includes sensitive information from users regarding their health. These are known as 'special categories of personal data' (Art 9 UK GDPR). Such information requires a higher protection than general personal data and there are certain conditions that must be met before special category data can be processed. The conditions which the Company can rely on in order to collect special category data are for health reasons and if the users have given explicit consent for the Company to collect and process that special category data for the intended purpose.

It is also important to stress that it is the Company's responsibility as a controller to ensure that appropriate technical and organisational measures are carried out in order to ensure that all data, including special category data, is stored, and processed safely. Please refer to page 4 of the advice letter under "Who is a Controller" for details of those specific technical and organisational measures.

When finalising the privacy policy, you should state (in "The type of personal information we collect" section) that you will be collecting special category health data. More information on special categories of personal data can be found here:

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/

Who is a Controller?

Art 4(7) UK GDPR defines a controller as a "*natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data*".

In this case, the Company is the controller and is responsible for determining how the information collected is processed and used. As the controller, the Company must comply with the obligations set out in the UK GDPR regarding the handling of personal data. This includes:

- Ensuring that appropriate technical and organisational measures are carried out within the Company where data processing is concerned and complying with the UK GDPR and other data protection laws. These 'appropriate' measures depend on a range of factors, including whether the data being processed is sensitive personal data such as health data. Organisational measures may involve staff training on all things data protection (Art 24 UK GDPR). Other technical measures include ensuring all users adopt a two-factor authenticator. This means that in addition to a username and password, users will also have to provide a one-time code which would be sent to them by SMS (in most cases) in order to login to their account.

- Following appropriate data protection policies when handling data. For instance, personal information such as payment card information should be deleted after a specified time. However, if the Company plans to use a third-party payment provider, then any payment card information would likely not be held by the Company.

- Informing the appropriate supervisory authority, the Information Commissioner's Office ("**ICO**"), within 72 hours of becoming aware of a data breach and the data subjects especially if it results in high risk (Art 33 & 34 UK GDPR).

- Ensuring that all individuals (data subjects) can exercise their rights regarding the collection and use of their personal data.

- Payment of data protection fees which will depends on the size and turnover of the Company. There are three tiers of fees: from £40 to £2,900. More information on data protection fees can be found on page 6 of this advice letter.

More information about the obligations of the controller can be found here:

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/controllers-and-processors/

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/how-do-you-determine-whether-you-are-a-controller-or-processor/

Who is a Processor?

Art 4(8) UK GDPR defines a processor as "*a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*". The processor operates under the authority of the controller and processes the data on instruction of the controller.

Processing includes any operation which is performed on personal data (Art 4(2) UK GDPR). It includes almost anything you do with data such as collecting, recording, storing, using, analysing, combining, disclosing or deleting it.

As such, [Confidential] and [Confidential] will be processors if they are processing personal data on behalf of the Company, as will any other external party that is used by the Company to process the personal data collected by them.

Who are Data Subjects? ("Users")

A data subject is defined as a *"natural identifiable person"* (Art 4(1) UK GDPR). In simple terms, they are people whose information is collected for the purpose of the Company and its operations. In this case, the data subjects are the users suffering from [Confidential] who are signing up via the App. They are the main users of the Company's platform and will have to provide personal data for full access. As such, they are afforded rights under the UK GDPR. It is therefore the responsibility of the controller (i.e., the Company) and processors ([Confidential] and [Confidential]) to ensure that these rights are respected when in possession of their personal information.

Some of the rights of data subjects include the right to:

- Be informed about the collection and use of their personal data. The Company must tell users: (i) whether data is obtained direct from the users themselves, or from a third party (such as payment service providers); and (ii) who the Company is giving the users' information to.
- Rectify any inaccurate personal information collected.
- Access the personal information collected from them.
- Have their information deleted.
- Restrict the use of their personal data.
- Request that their personal data be transferred from one organisation to another.
- Object to the use of their personal data.

These rights are listed in the "Your Legal Rights" section of the template privacy policy. More information about the rights of data subjects can be found here:

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

Personal Information Shared with Third Parties

The Company will be sharing data in a number of different ways with different parties:

1. Sharing data with other controllers (for example third party payment service providers) and processors (including [Confidential] and [Confidential]).

2. Sharing data by providing access to the third-party App developer.

3. Sharing of data within the UK and abroad.

If the information is shared with parties within the UK and EU, the Company must comply with the obligations contained in Art 5(1) UK GDPR regarding the handling of personal data. It is important to note no additional safeguards or procedures are needed when sharing data with third parties in the EU. This is because the UK considers the EU "adequate" which means data can flow freely between to the UK and EU, while being in accordance with UK data protection laws.

However, if the Company shares information with third parties outside the UK and EU, it must also comply with the provisions in Art 44-50 UK GDPR. In these circumstances, the Company may be required to put a contract in place with the third party, especially if that third party is located within the USA.

If you require specific advice on this issue of sharing data with third parties outside of the UK and EU, then please contact lawyers in those jurisdictions directly for assistance, as this issue falls outside the scope of our advice.

As mentioned previously, the Company will be sharing information about individuals with [Confidential] and [Confidential]. As such, the Company is required to notify the data subjects about when their information is shared with third parties. The Company must notify the users before the information is shared with those third parties and should include this information in the "Disclosures of your personal data" section in the privacy policy.

You also mentioned that the Company does not have a contract with the App developer. We recommend that a contract is drawn up between the developer and the Company, as the Company could potentially be in breach of UK GDPR because the users' personal data can be accessed by a third party. We strongly recommend that you contact lawyers to seek further advice on this matter. In any event, details of the third party should be set out in the Company's privacy policy.

What is the Data Protection Fee?

Under the Data Protection (Charges and Information) Regulations 2021, the Company is required to pay a data protection fee to the UK data protection authority, which is the ICO, because it processes personal data. The data protection fee must be paid annually, and will be:

- £40 if the Company has a maximum turnover of £632,000 for the financial year or no more than 10 members of staff ("**Tier 1**").

- £60 if the Company has a maximum turnover of £36 million for the financial year or no more than 250 members of staff ("**Tier 2**"); or

- £2,900 if the Company does not meet the criteria for Tier 1 or Tier 2 ("**Tier 3**").

We believe that the Company falls into Tier 1 and therefore the data protection fee will be £40 (£35 if the fee is paid by direct debit), but you can confirm the Applicable fee tier by yourself at: https://ico.org.uk/for-organisations/how-much-will-i-need-to-pay/

To confirm whether the Company is obligated or exempt from paying the data protection fee, you can use the self-assessment checker available on the ICO website at https://ico.org.uk/for-organisations/data-protection-fee/self-assessment/. If not exempt, you can register and proceed with the data protection fee payment at: https://ico.org.uk/registration/new.

Does the Company need to appoint a Data Protection Officer?

The UK GDPR introduces a duty for certain companies to appoint a Data Protection Officer ("**DPO**"), including companies which are classified as public authorities or carry out certain types of processing activities. DPOs inform and advise on a company's data protection obligations and act as a contact point for users and the ICO. A DPO can be an existing employee or can be externally appointed.

We believe that currently the Company does not need to appoint a DPO as the Company's core activities do not consist of large-scale processing of special categories of data. For confirmation of this, you can use the self-assessment checker available on the ICO website at https://ico.org.uk/for-organisations/does-my-organisation-need-a-data-protection-officer-dpo/. More information on DPOs can be found at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/#ib1.

Templates

You have asked us to provide a template privacy policy and cookie policy for the website and App. We have attached a document containing this information in a separate file which you can tailor to the needs of the Company.

Privacy Policy

The privacy policy provides clear, transparent, and easily accessible information about how the Company uses data subjects' information and rights on the website and App. You can find more information about privacy policies on the ICO website at:

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/.

Cookie Policy

A cookie is a small text file that is downloaded to a device (usually a computer or smartphone) when a user accesses a website. It allows the website to recognise that user's specific device and store some information about the user's past actions and preferences.

The cookies requirement for websites arises under the PECR. The PECR requires that cookie information must be clear and comprehensive. Information about how the specific cookies work and what they are used for are needed so that users can understand the potential consequences of allowing cookies to be downloaded to their devices.

More information about the PECR and cookies can be found on the ICO's website at:

https://ico.org.uk/for-organisations/guide-to-pecr/cookies-and-similar-technologies/
https://ico.org.uk/for-organisations/guide-to-pecr/what-are-pecr/

The cookie policy attached provides clear and comprehensive information about cookies. It sets out which cookies the Company currently uses on the website, the purpose for which they are used and how users can opt-out or manage their cookie preferences. Please note that cookie policy should be updated accordingly if the cookies used by the Company change.

Next Steps

- Based on the information collected, you are advised to evaluate the Company's practices ensuring that the collection and use of personal information from users complies with the regulations under the UK GDPR.
- The Company should consider employing a DPO to oversee the process of handling the personal data collected, especially if "special category data" is planned to be processed on a large scale in the future.
- You should tailor the templates to suit the preferences of the Company.
- If the Company changes the manner in which it uses the data collected, the privacy policy will have to be updated to ensure that the data subjects are informed as to how their information is being used.
- The Company should have a contract with the App developer to ensure that the user data being shared with the App developer is not in breach of the UK GDPR.

We hope that the advice provides you with a comprehensive understanding of the legal questions you asked us to address. Should you require any assistance in any future matters, please do not hesitate to contact us.

Yours sincerely,

[Confidential]
Student Adviser

[Confidential]
Student Adviser