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]

21 March 2022

PRIVILEGED & CONFIDENTIAL

By email to: [Confidential] and [Confidential]

Dear [Confidential] and [Confidential]

Re: Your appointment with qLegal on Tuesday 22 February 2022.

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.

SUMMARY OF THE FACTS AND DOCUMENTS YOU HAVE PROVIDED

You are developing a service marketplace for connecting [Confidential] practitioners with users (the "**Business**"). The Business will offer services to under 18s after the first three months of launching. Children will be able to use the services by linking their profile to that of a parent. In this way, parents can give permission for use of the services. A linked parent and child account would have access to the same content. The Business does not have an existing insurance policy and has not finalised its Terms and Conditions or Privacy Policy.

We have been provided with the following documents:

(i) Guidelines: Working with children and young people within the [Confidential] professions;
(ii) Updated Legal Brief – GDPR Guidance;
(iii) Turnover Projection.

SCOPE OF OUR ADVICE

You want to understand whether you are sufficiently compliant with data protection law, specifically:

Data Subject Access Requests ("DSARs")

(i) What information would you need to provide to users making a DSAR? Specifically, how would this apply to practitioners' private notes made after a consultation?
(ii) What information would need to be provided to a parent or guardian if they requested data about their dependent?

Admin staff ("Admin") and support staff ("Support") access

(i) Do you need to remove or restrict Admin and Support's ability to sign into users' and practitioners' accounts?
(ii) What information should Admin and Support have access to?

Under 18s and consent

(i) Is your proposed approach to obtaining informed consent from under 18s sufficient?

Data breaches

(i) How should you respond to a data breach?
(ii) Should you purchase specific insurance which covers data breaches?

Terms and Conditions and Privacy Policy

(i) Are your current Terms and Conditions and Privacy Policy sufficient, particularly regarding under 18s?

Further considerations

(ii) Do you need a third party to review your compliance before you launch the website?

SUMMARY OF ADVICE

DSARs

(i) In the event of a DSAR, the private notes made by a practitioner may only be revealed to the user at the discretion of the practitioner or if the information is already known to the individual.
(ii) DSARs regarding a dependent will follow the same procedure unless they fall under one of the exemptions under the UK General Data Protection Regulation (the "**UK GDPR**").

Admin and Support access

(i) According to data protection by design and default principles, Admin and Support should only have access to accounts when it is necessary to the function of their job and only be privy to information relevant to them.

Under 18s and consent

(i) We cannot advise on the sufficiency of your approach to obtaining informed consent to [Confidential] for under 18s. This is a regulatory, and not a data privacy, law issue and is therefore outside the scope of our work.

(ii) Relying on consent as a lawful basis for processing personal data, particularly for under 18s, is not advisable. It would be better to rely on alternative legal bases, e.g. because processing is necessary for entering into and performing contracts with users of the platform, and for providing health treatment.

Data breaches

(i) You should document the breach, take steps to remedy it and assess the risks it poses to the affected individuals. If the breach is high risk, you will need to inform the affected individuals and/or the Information Commissioner's Office (the "**ICO**"). You should also consider implementing security measures to mitigate any future breach.

(ii) Whilst we are not insurance law specialists and have not taken insurance advice, we ultimately consider that it is a commercial decision whether you wish to purchase data breach insurance. Public Liability Insurance ("**PLI**") and Employers' Liability Insurance ("**ELI**") should cover claims and the costs of actions against you. You may want to purchase data breach insurance to cover additional costs, but it is not clear that ICO fines can be insured against under English law.

Terms and Conditions and Privacy Policy

(i) Since you do not have current Terms and Conditions or a Privacy Policy, we refer you to resources to assist with drafting these.

Further considerations

(i) You are not obliged to have a third party review your data protection compliance before you launch the website. However, you should consider that you have further data protection obligations outside of the scope of this advice and you may want to take further advice on these points.

EXPLANATION

Our advice is limited to your obligations under the UK GDPR and the Data Protection Act 2018 (the "**DPA**"). We have not considered regulatory or insurance law.

What are the key data protection concepts you should be aware of?

(i) ***Data Controller*** – The Business determines the purposes and means of processing because it has control of the platform, including what personal data is being processed, how and why. It is therefore a data controller with obligations under data protection law.

(ii) ***Personal Data/Data Subject*** – Personal data is any information relating to an identified or identifiable individual, i.e. a data subject. Personal data is broadly defined and includes a person's name, email address, their image or their voice. It is essentially any information which could identify the person.

(iii) ***Sensitive or Special Category Data*** – Since the Business is a platform for practitioners and users, it will be processing sensitive or 'special category' personal data. Genetic, biometric and health data, in addition to data about a person's sex life or sexual orientation are all categories of sensitive personal data. Processing this data requires additional protections.

(iv) ***Processing*** – 'Processing' means any operation performed on personal data. The Business will process personal data when it collects, uses, discloses or retains it. Even simply storing personal data in an electronic filing system constitutes processing.

(v) ***The ICO*** – The ICO is the UK data protection authority and regulator, responsible for enforcement. The ICO can issue fines to data controllers who fail to comply with their obligations. The ICO may investigate data controllers as a result of a data breach or a complaint made by a data subject. Data subjects can also issue claims against data controllers, particularly arising from data breaches.

DSARs

What information would you need to provide to users making a DSAR?

Individuals have a right of access, meaning they are entitled to ask whether you are processing their personal data and to have copies of that data. The following is a comprehensive list of information which individuals have the right to obtain from a controller (much of which is generally included in the Privacy Policy):

(i) Confirmation that you are processing their personal data;
(ii) A copy of their personal data;
(iii) Other supplementary information;
(iv) Your purposes for processing;
(v) Categories of personal data you are processing;
(vi) Recipients or categories of recipient you have or will be disclosing the personal data to (including recipients or categories of recipients in third countries or international organisations);
(vii) Your retention period for storing the personal data or, where this is not possible, the criteria for determining how long you will store it;
(viii) The individual's right to request rectification, erasure, or restriction or to object to processing (subject to specific conditions);

(ix) The individual's right to lodge a complaint with the ICO;
(x) Information about the source of the data, if you did not obtain it directly from the individual;
(xi) Whether or not you use automated decision-making (including profiling) and information about the logic involved, as well as the significance and envisaged consequences of the processing for the individual;
(xii) The safeguards you have provided where personal data has or will be transferred to a third country or international organisation.

Although much of this information should be included in your Privacy Policy, individuals still have the right, to request this information from you. In response to a DSAR, the information above should be supplied in conjunction with a copy of the personal data itself. Under the right of access, an individual is only entitled to their own personal data. They are not entitled to information relating to other people, unless:

(i) Their data also relates to other individuals; or
(ii) They are exercising another individual's right of access on their behalf (with the appropriate legislative authority and permission from the individual).

A list of exemptions regarding the right of access can be found here: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/right-of-access/what-other-exemptions-are-there/.

What are the restrictions on disclosing health data?

The DPA defines 'health data' as personal data relating to the physical or mental health of an individual, including the provision of health care services, which reveals information about their health status. Practitioners' notes made after a consultation can be regarded as 'health data'.

If you are not a health professional, you must not disclose health data in response to a DSAR, unless:

(i) Within the last six months you have obtained an opinion from the appropriate health professional that the serious harm test for health data is not met (you are exempt from complying with a DSAR for health data if doing so would be likely to cause serious harm to the physical or mental health of any individual); or
(ii) You are satisfied that the individual it is about has already seen, or knows about, the health data.

In the event of a user making a DSAR, practitioners' notes may therefore only be disclosed at the discretion of the practitioner or if the information in the notes is already known to the individual.

An overview of exemptions regarding health data can be found here: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/right-of-access/what-other-exemptions-are-there/.

What information would need to be provided to a parent or guardian if they requested data about their dependent?

Under the UK GDPR, there is an exemption from the right of access if you receive a request from someone with parental responsibility for an under 18 (or under 16 in Scotland). However, the exemption only applies when complying with the request would disclose information that:

(i) The individual had provided to you in the expectation that it would not be disclosed to the requester, unless the individual has since expressly indicated that they no longer have that expectation;
(ii) Was obtained as part of an examination or investigation to which the individual consented in the expectation that the information would not be disclosed in this way, unless the individual has since expressly indicated that they no longer have that expectation; or
(iii) The individual has expressly indicated should not be disclosed in this way.

Even if a child is too young to understand the implications of their rights, their rights are still vested in them, rather than their parent or guardian. You should therefore only allow parents to exercise rights on behalf of a child if the child authorises them to do so, when the child has insufficient understanding to exercise the rights themselves, or when it is evident that this is in the best interests of the child.

If you are satisfied that the child is not competent, and that the person who has approached you holds parental responsibility for the child, then it is usually appropriate to let the holder of parental responsibility exercise the child's rights on their behalf, unless you have evidence that this is not in the best interests of the child.

If you are confident that the child can understand their rights, then you should usually respond directly to the child. You may, however, allow the parent to exercise the child's rights on their behalf if the child authorises this, or again if it is evident that this is in the best interests of the child. This allows the child to withhold information from the parent should they see fit. In these cases, the same information would be provided as any other DSARs so far as the information has been approved by the child.

More information on parents and guardians requesting data for their dependants can be found here: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-uk-gdpr/what-rights-do-children-have/

Admin and Support access

Do you need to remove or restrict Admin and Support's ability to sign into users' and practitioners' accounts?

According to the UK GDPR there is a requirement to put in place appropriate technical and organisational measures to implement the data protection principles effectively and safeguard individual rights. This is 'data protection by design and by default'. This requires considering data protection and privacy issues as paramount in every process. It can help you ensure that you comply with the UK GDPR's fundamental principles and requirements, and forms part of the focus on accountability.

Therefore, to adhere to an individual's right to privacy it would be best to design the system in a way that restricts Admin and Support's ability to sign into users' and practitioners' accounts, unless it is deemed

necessary, or design the system in a way such that each stakeholder is only privy to information necessary to complete their function.

More information on data protection by design and default can be found here: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/.

Under 18s and consent

Is your proposed approach to obtaining informed consent from under 18s sufficient?

It is important to distinguish between consent to data processing and consent to medical treatment. Whether an under 18 is competent to consent to [Confidential] is an issue in medical law and is outside the scope of the advice we can give you. Consent is a consideration in data protection law because it is one of an array of lawful bases for processing data. All processing of personal data must have a lawful basis. Processing sensitive personal data requires an additional specific basis for processing. Data subjects must be informed about the bases for your processing of their data. This information should be included in your Privacy Policy.

Under the UK GDPR, consent has a high threshold for validity and therefore is not a strong basis to rely upon for processing. Conditions must be met for consent to be valid; it must be freely given, specific, informed and unambiguous. It is a less appropriate basis for processing the data of children. They may have difficulty understanding how their data will be used, resulting in uncertainty about whether they have given truly informed consent. Consent can also be withdrawn at any time, meaning that any dependent processing must cease. We therefore do not advise that the Business relies on consent as the basis for processing either child or adult personal data.

Better alternative bases, which would be available to you, would be that the processing is necessary for entering into a contract or necessary for the Business's legitimate interests. As explained above, processing sensitive personal data requires an additional legal basis. Again, you do not need to use consent as this basis for processing but can rely on the basis that you need to process sensitive personal data in order to provide health treatment. The ICO refers specifically to the lawfulness of providing online counselling services to children on this basis, without the need for consent: https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/children/#4.

Although we do not anticipate that under 18s' consent to data processing will be necessary for you to consider, you may want to consider other data protection issues presented by under 18s. We refer you to this very clear summary of considerations for processing child data, which are set out in full in the ICO's Children's Code: https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/code-standards/.

Data breaches

How should you respond to a data breach?

A personal data breach is a security incident whereby personal data is compromised in respect of confidentiality, integrity or availability. For example, personal data might be compromised by accidental or unlawful destruction, loss, alteration, disclosure or inaccessibility.

In the event of a breach, you should take steps to remedy it. These steps will depend on the nature of the breach. If personal data has been disclosed inadvertently, you should ask any unintended recipients to delete the data they have received. You must also document the breach, including information about the causes, facts, effects and remedial action taken.

Additionally, you must consider whether you need to notify the ICO and the affected data subjects. This will depend on an assessment of the risks posed by the breach. You must notify the ICO of a breach unless it is unlikely to pose a risk to the rights and freedoms of data subjects. Conversely you would only need to notify the affected subjects of a breach if it was likely to result in a high risk to their rights and freedoms. Even in the case of high risk, you may not need to notify the affected subjects if an exception applied, (for example, where the data was encrypted).

The assessment should be specifically of risk, resulting from the breach, to subjects' rights and freedoms. A breach presents risks when it may cause physical, material or non-material damage. Examples include: loss of control of data, limitation of rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data subject to professional secrecy and economic or social disadvantage.

The assessment should also consider the likelihood and severity of the risks. These can be determined by examining: the type of breach, nature, sensitivity and volume of data, ease of identification, severity of consequences, special characteristics of the individual or of the controller and the number of affected subjects. Given that the Business facilitates therapy sessions, it is likely that any future data breach it experiences may involve health data, in which case, damage is likely. Assessing risk must be conducted on a case-by-case basis, however.

If notification is required, you should do so without undue delay and, in the case of the ICO, within 72 hours of realising the breach. The notification should detail: the nature of the breach, including the categories and number of subjects and data records concerned; the data protection officer's name and contact details; the likely consequences of the breach; and measures to address or mitigate the breach. For the benefit of data subjects, this information must be given in clear, plain language.

You should generally have appropriate data security, including technical and organisational measures for preventing data breaches. You should adopt measures implementing privacy by design and by default. For example by minimising the volume of data you collect and by processing it with the utmost security. You should also regularly evaluate your privacy policies and train staff on privacy, handling data and avoiding common data breaches. There is not a comprehensive list of the possible measures you could take.

Should you purchase specific insurance which covers data breaches?

PLI should cover you for any third party claims, including those arising from a data breach. But you would need to check the exact provisions of any insurance policy you purchase. You should ensure it covers your legal costs as well as those of other parties. Since PLI might only cover third party claims, you may also want to consider ELI, in case of claims by employees whose data is subject to a breach.

You can purchase data breach insurance, although there is no legal obligation for you to do so. This can help with covering the cost of notifying affected data subjects and/or the ICO, or cover the cost of any PR campaign regarding the breach. It is a matter for you whether you want to purchase this level of cover.

It is unclear, however, whether you can, under English law, insure against regulatory fines and penalties, such as might be imposed by the ICO for non-compliance with data protection law. This issue is yet to be tested in English courts. But it is probable that they are not insurable. This is because regulatory fines, which serve a punitive purpose, cannot be insured. The punitive effect would be negated if the fine were simply covered by insurance. ICO fines could be said to have some punitive purpose and therefore possibly fall into this category of uninsurable penalties.

Terms and Conditions and Privacy Policy

Are your current Terms and Conditions and Privacy Policy sufficient, particularly regarding under 18s?

Website Terms and Conditions inform users about their rights and obligations in using the Business's services. They should identify the parties to the agreement, the Business's services, and measures to be taken in the event of a problem arising. Additionally, the Business should display a Privacy Policy on its website as part of its obligation as a data controller to process data transparently. Since you explained that you do not have existing Terms and Conditions or a Privacy Policy, we advise that you draft these documents with reference to the following resources, which include a very accessible template Privacy Policy and a list of what should be included in your Terms and Conditions:

http://www.qlegal.qmul.ac.uk/media/qlegal/docs/What-to-Consider-When-Creating-a-Website-for-Your-Business.pdf
https://ico.org.uk/for-organisations/make-your-own-privacy-notice/
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/what-privacy-information-should-we-provide/

Further considerations

Do you need a third party to review your data protection compliance before you launch the website?

There is no legal obligation to have a third party review your data protection compliance before launching your website. But you should consider taking further advice on your additional data protection obligations, which are outside of the scope of our advice above. For example:

(i) *Data protection fee/registration with the ICO* – Since you are a data controller, you must register as such by paying a data protection fee to the ICO (https://ico.org.uk/for-organisations/data-protection-fee/).

(ii) *Data protection officer ("**DPO**")* – Data controllers which process special category data on a large scale must have a DPO. This likely applies to the Business. The ICO website gives further guidance (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/).

(iii) *Joint controller, processor and data sharing agreements* – The Business may at times be a joint controller with or even a processor for practitioners on the platform. To gain certainty about which party is responsible for which data protection obligations, you may want to use a joint controller agreement, a processor agreement and a data sharing agreement as part of your contracts with practitioners. For further explanation of these concepts, please see:
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-does-it-mean-if-you-are-joint-controllers/;
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/accountability-and-governance/contracts/
https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/data-sharing-a-code-of-practice/data-sharing-agreements/
https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/data-sharing-a-code-of-practice/data-sharing-covered-by-the-code/#organisation

(iv) *Subject rights* – The right to access is only one of several rights vested in data subjects (more information is available here: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/).

(v) *Data Protection Impact Assessment ("**DPIA**") and Legitimate Interests Assessment ("**LIA**")* – You will likely need to complete a DPIA because you will be processing health data, which is potentially high risk (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/). In order to rely on legitimate interests as a basis for processing, you will need to conduct an LIA (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/).

The ICO website is an accessible resource for information about your obligations as a data controller (https://ico.org.uk/for-organisations/). They also have a very useful helpline, where you can seek specific advice on data protection issues (0303 123 1113).

NEXT STEPS

1. Anticipate data breaches, including the following steps:
   a. Set out a clear policy for dealing with breaches, as per our advice above;
   b. Prepare template letters in the event that the affected data subjects and/or the ICO need to be notified;
   c. Protect personal data, particularly sensitive health data, and, as appropriate, encrypt and anonymise data;
   d. Implement privacy by design and by default;
   e. Regularly evaluate your privacy policies;
   f. Train staff on privacy and data protection.

2. Draft your Privacy Policy and Terms and Conditions;

3. Research the full extent of your data protection obligations and consider taking further advice on these.

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.

We would be extremely grateful if you could take a few moments to complete this short form https://qmul.onlinesurveys.ac.uk/client-feedback-on-qLegal-2021-22, as your feedback is important to our educational development and the development of our services.

Yours sincerely,

[Confidential] [Confidential]

Student Adviser **Student Adviser**

On behalf of qLegal