Information Security terms for experts and third parties

You are a data controller in respect of the personal data that we provide to you in connection with these instructions. This is because you determine what information you require from us in order to deal with our instructions and the manner in which you will process that information. You are also responsible for the content of the information that you provide to us in dealing with our instructions. Browne Jacobson is made up of Browne Jacobson LLP, Browne Jacobson Ireland LLP, Browne Jacobson (VI) Limited, Browne Jacobson Northern Ireland Limited, Mowbray Trustees Ltd and Mowbray Trust Corporation Ltd. When we mention 'Browne Jacobson', 'we', 'us' or 'our' in these terms, we are referring to the relevant business connected with this instruction.

1. In accepting these instructions you agree that you are a data controller in respect of the personal data you receive from, and send to, us in connection with those instructions and will comply with applicable data protection legislation (which for the avoidance of doubt may include the Data Protection Act 2018, UK GDPR, the EU GDPR and/or any other applicable legislation that relates to data protection or privacy of communications) and guidance at all times when processing that data.

2. You warrant and undertake that:

   a) where you provide personal data to us, you have the consent of the relevant data subject to do so or have satisfied yourself that such consent is not a legal requirement;

   b) you will only use the information we provide to you ("the Shared Data") for the purposes of dealing with these instructions and for no other purpose;

   c) you will not disclose any of the Shared Data to a third party without our prior written consent, which will not be unreasonably withheld or delayed but may be granted subject to conditions such as that you will use all reasonable endeavours to ensure that that third party is bound by obligations equivalent to those imposed on you by these terms and by applicable data protection legislation;

   d) you will not retain any of the Shared Data for longer than is necessary to deal with these instructions and at the end of that period you will securely destroy the Shared Data save where we have indicated that information should be returned to us in which case you will return that information to us by secure means;

   e) where you are based in the European Economic Area (EEA), you will not transfer the Shared Data outside of the EEA without our prior written consent;

f) where you are based in the UK, you will not transfer the Shared Data outside the UK without our prior written consent;

g) any communications you have with us that contain personal and/or confidential information shall be transmitted in a secure manner such as by way of encrypted emails or attachments or a data room established and operated by us;

h) you will use appropriate technical and organisational measures to ensure compliance with applicable data protection legislation and to protect the Shared Data against unauthorised or unlawful processing and against accidental loss, destruction or damage;

i) you will limit printing of Shared Data to the minimum required. The routine printing of Shared Data is strongly discouraged. Any printed copies will be held securely as set out in (j) below and confidentially destroyed once they are no longer required, which for the avoidance of doubt requires the use of external contractors who provide a certificate of destruction (to be provided to us on request);

j) the Shared Data will be kept safe at all times (including, but not limited to, allowing only authorised individuals to have access to the printed or electronic records that contain the Shared Data; the Shared Data not being left unattended in non-secure areas; any hard copy documents being kept in a secure space such as a lockable cabinet; not saving documents on a network device that is accessible by unauthorised individuals);

k) where any of the Shared Data is carried on an electronic device (e.g. a laptop or iPad) or can be accessed from any mobile device, that device is encrypted and you will take appropriate steps to ensure that the Shared Data remains safe (for example by way of the use of virus protection measures) and all Shared Data saved to a device is digitally destroyed before the device is disposed of or sent out for repair;

l) as soon as is reasonably practicable you will notify us of any actual or potential breach of these terms or the applicable data protection legislation and any steps taken by you in relation to that actual or potential breach and liaise with us in relation to those steps. This means that you will inform us immediately if there is any loss of the Shared Data or if you have reasonable grounds to suspect that any of the Shared Data could have been accessed and/or viewed by any unauthorised third party and you will take all necessary steps to retrieve lost data and/or mitigate the effects of such loss;

m) as soon as is reasonably practicable you will notify us of any request received by you from a data subject for access to any personal data contained within the Shared Data and of any requests for the rectification or erasure of any such personal data or for the restriction of processing of any such personal data and liaise with us as to the response to be made to such requests;

n) as soon as is reasonably practicable you will notify us of any actual or potential claim of which you become aware or any complaint to or investigation by a regulatory authority that relates to your processing of the Shared Data and liaise with us as to the response to be made to that actual or potential claim, complaint or investigation;

o) you will provide reasonable assistance and co-operation to us in respect of any of the matters referred to at paragraphs 2.k and 2.l above that we receive and of which you are notified; and

p) you will indemnify us for any cost, charge, damages, expenses or losses caused as a result of any actual or potential breach of these terms and/or the applicable data protection legislation for which you aredirectly or indirectly responsible.

3. In the event that the transfer of personal data between you and us is a transfer which would be prohibited under the data protection legislation in the absence of approved standard contractual clauses, then

a) in relation to personal data that is protected by the EU GDPR, the standard contractual clauses approved by the European Commission ('EU SCCs') shall apply as follows:

– Module One will apply;

– in clause 7, the optional docking clause will apply;

– in clause 11, the optional language will not apply;

– in clause 17, Option 1 will apply, and the EU SCCs will be governed by Irish law;

– in clause 18(b), disputes shall be resolved before the courts of Ireland;

– the data exporter shall be us and you shall be the data importer;

– Annex I of the EU SCCs shall be deemed completed with the information set out in the Processing Details.

– Annex II of the EU SCCs shall be deemed completed with the information set out in the Processing Details.

b) in relation to personal data that is protected by the UK GDPR, the standard contractual clauses approved by the UK government ('UK SCCs') shall apply as follows:

– the EU SCCs shall apply, completed as set out above in clause 3a above

– the UK Addendum to the EU SCCs issued by the Information Commissioner's Office under s.119A(1) of the Data Protection Act 2018 ("UK Addendum") shall be deemed executed between us and you, and

– the EU SCCs shall be deemed amended as specified by the UK Addendum in respect of the transfer of such personal data.

In processing personal data in connection with these instructions, you are not acting as the employee or agent of Browne Jacobson we are not acting as joint data controllers with you and no partnership is created.

For the avoidance of doubt, your continued dealing with us will amount to acceptance of these terms.

Data Processing Details:

Nature and purposes for which the Personal Data shall be processed	For the purpose of the provision of the services by one party to the other. This may include for the provision of services by Browne Jacobson to its client or by a third party to Browne Jacobson, depending on the particular circumstances.
Description of the categories of the data subjects	As set out in any main agreement between the parties or as otherwise transferred between the parties.
Description of the categories of Personal Data (including sensitive data if applicable). If sensitive data, details of applied restrictions	As set out in any main agreement between the parties or as otherwise transferred between the parties.
The envisaged time limits for erasure of the different categories of Personal Data	See Data Retention Schedules
Frequency of transfer	Continuous
Competent Supervisory Authority	Where the UK GDPR applies, UK, Where the EU GDPR applies, Ireland
Technical and Organisational Security Measures	• Information security and data protection policies and procedures; • Ongoing awareness programme and training for staff covering data protection and information security (including cyber risk); • Information classification labelling and secure storage and access; • 'Paper light' approach where documents received are stored within secure electronic filing systems and hard copies only retained where absolutely necessary;

	• Use of secure data rooms for the exchange of information where appropriate; • Device encryption and multi-factor authentication protocols, where agreed, with restrictions on use of USB sticks/removable devices; • Malware and antivirus protection; • Routine testing of the security of IT systems