10. Social Network Application

If user uses any of our social network applications, pages or plugins or user use one of our products or services that allow interaction with social networks, we may receive information relating to user social network accounts. For instance:

a) If user log-in to one of our websites or services using user social network account, we may receive basic details from user social network profile. The basic details we receive may depend on user social network account privacy settings. They might include user social network ID, name, profile picture, gender and locale. We may also receive additional information from user profile if user give us permission to access it.

b) If user click on a 'like', '+1' or 'tweet' or similar button in one of our websites or services, we may record the fact that user have done so. In addition, the content that user is viewing may be posted to user social network profile or feed. We may receive information about further interactions with this posted content (for example, if user contacts click on a link in the posted content), which we may associate with the details that we store about the user.

c) If user 'like', '+1' or similar one of our pages on a social network site, we may receive information about user social network profile, depending on user social network account privacy settings.

For more information and details about how user can control access to their social network profile, user should view the privacy policy and other guidance available on their social network's website.

11. Data Security

We take appropriate and commercially reasonable technical, physical, and administrative measures to protect personal data from misuse or accidental, unlawful or unauthorised destruction, loss, alteration, disclosure, acquisition or access in accordance with applicable laws. These processes and systems include:

a) Limiting access to the information and using identity and access management technologies to control access to systems on which information is processed and stored.

b) Putting in place physical, electronic and procedural safeguards in line with industry standards.

c) Requiring all TA employees to complete training about information security.

d) Monitoring and regularly reviewing our practise against our own policies and against industry best practice.

e) Third party appointed by us for processing the personal data is bounded to meet the relevant requirements of PDPA and acceptable security measures are implemented to protect the confidentiality of the personal data.