● Which of the standards discussed in the sources above would apply to the website/ organisation assigned to you for the assessment? For example, a company providing services to anyone living in Europe or a European-based company or public body would most likely be subject to GDPR. A company handling online payments would most likely need to meet PCI-DSS standards.

The website my group was assigned is a blog site. It would be required to follow the GDPR as a site that is based in the UK. The website can hold personal information about individuals such as names, email, location, or other personally identifiable information (ICO, 2020). The website does not do online payments, so it does not need to meet PCI-DSS standards.

● Evaluate your assigned website against the appropriate standards and decide how you would check if standards were being met?

One of the first ways to check if the standards are being met is to use a GDPR checklist. The checklist would be a systematic walkthrough, that checks each aspect of a business for compliance in the different categories (GDPR.EU, 2020). As well one with access to data should know about the GDPR make such any changes are within compliance.

● What would your recommendations be to meet those standards?

Given the size of the website, the most affordable and practical way to meet the standards would be the use of a third-party compliance company. That way the complex requirements could be offloaded to someone else, with significantly more knowledge. As well it could save money by not needing to have a data controller to regularly monitor the website.

● What assumptions have you made?

Several assumptions have been made. The first assumptions are that the GDPR is the only standard that applies to the website. As well it is assumed that the website doesn’t have a data processor to monitor it for GDPR compliance. However, given the size of the website, it would seem very unlikely for that to be true.

References:

GDPR.EU (2022) Everything you need to know about GDPR compliance. Available from: <https://gdpr.eu/compliance/?cn-reloaded=1> [Accessed 19 January 2022].

ICO (2020) Guide to the General Data Protection Regulation (UK GDPR). Available from: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/> [Accessed 18 January 2022].