schellman
Quality. above all.

Microsoft Supplier Security and Privacy Assurance (SSPA) Program Attestation

If your organization is a current or aspiring Microsoft vendor, you're probably familiar with the Microsoft SSPA program. Vendors providing services with a high business impact may be required to provide a letter of attestation from a qualified independent assessor such as Schellman.

Let's look into what this requirement means for your business and what to expect during the attestation process.

WHITEPAPER

Choosing an Independent Assessor

Choosing an assessor with experience and understanding of privacy principles is a great start, but there are a few more qualifications to look for:

- The attestation should be performed in accordance with the guidelines provided by Microsoft and by a preferred assessor listed on the Microsoft SSPA website.
- As Microsoft's vendor contracts are heavily affected by the European Union's new privacy law, the GDPR, a qualified assessor should have experience with both US and European privacy attestations and audits.
- Look for a firm whose auditors hold privacy-specific certifications such as the CIPP/E and CIPP/US by IAPP.

WHITEPAPER

schellman
Quality. above all.

Completing the Attestation Process

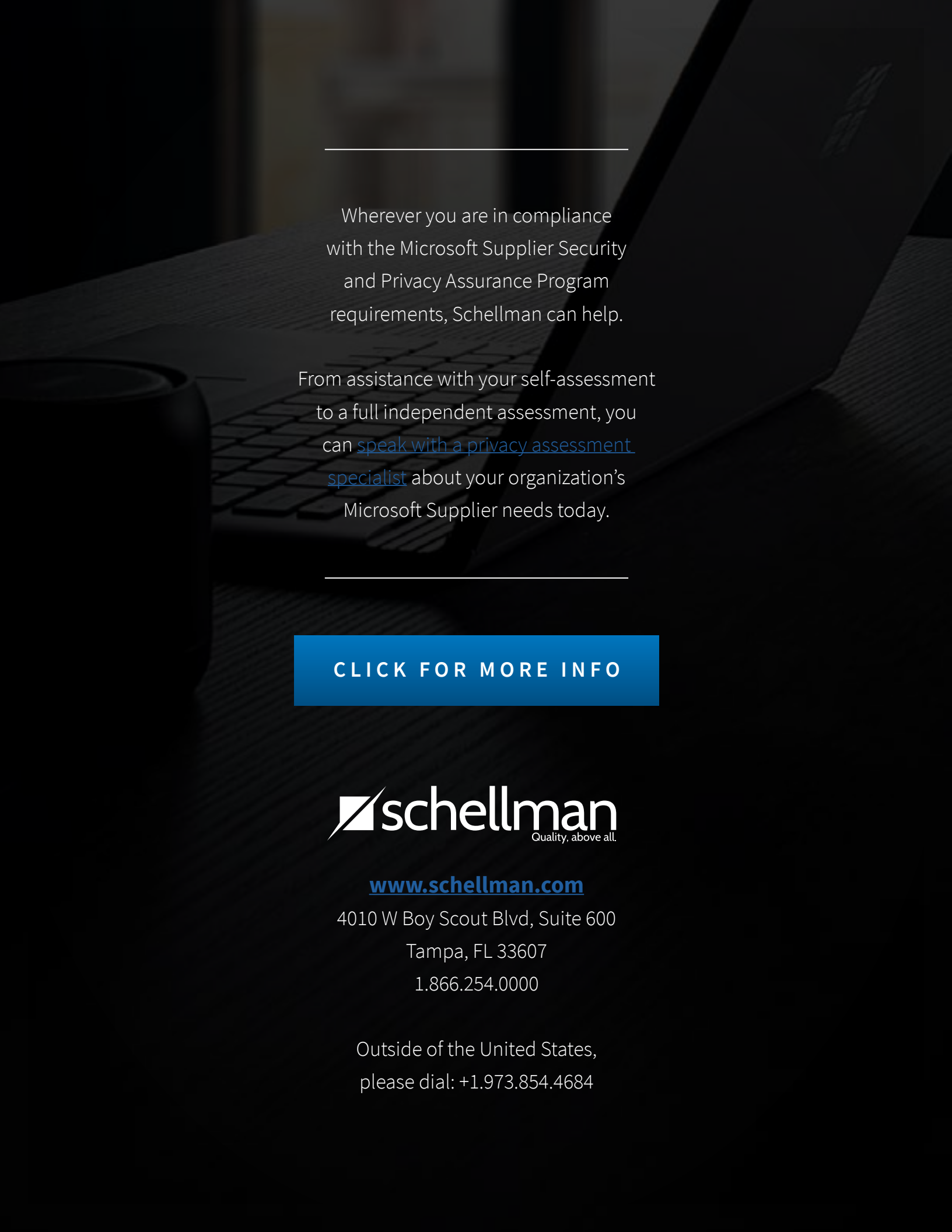
All Microsoft vendors are required to be compliant with the SSPA and provide a self-assessment against their DPR. Some vendors will be selected by Microsoft to also verify compliance with the DPR by an independent assessment.

Therefore, before the attestation, check the Data Protection Requirements (DPR) and make any necessary changes to meet the criteria. During the independent assessment, your auditor will ask for some evidence to show that you've met these requirements, so be sure to keep some documentation of your work and controls. When the assessment is complete, you'll be given a letter of attestation which you can submit to Microsoft.

"Your auditor can point out areas for improvement and help you identify weaknesses in your current practice to avoid jeopardizing your Microsoft contract.

With Schellman as the assessor, your auditor can point out areas for improvement and help you identify weaknesses in your current practice to avoid jeopardizing your Microsoft contract. If your organization is subject to other types of IT audits, discuss the option of combining the Microsoft DPR attestation with other audits or assessments to determine if there is an overlap in testing efforts or documentation to ease the burden of multiple audits.

If your organization has completed a SOC 2 or currently holds an active ISO 27001 certificate, the scope of the assessment could be reduced.



Wherever you are in compliance with the Microsoft Supplier Security and Privacy Assurance Program requirements, Schellman can help.

From assistance with your self-assessment to a full independent assessment, you can speak with a privacy assessment specialist about your organization's Microsoft Supplier needs today.

CLICK FOR MORE INFO

schellman
Quality, above all.

www.schellman.com
4010 W Boy Scout Blvd, Suite 600
Tampa, FL 33607
1.866.254.0000

Outside of the United States,
please dial: +1.973.854.4684