	SAAS PROVIDER SECURITY CHECKLIST
□	Regarding SaaS data protection, is the vendor able to perform fast, accurate point-in-time restores - and to do so at scale? (When testing, you may wish to assess against more than a small demo set of data.)
□	Does the vendor enable end users to restore the data they have permission to edit? Watch this video to learn about the value provided by accurate point-in-time restores for end users.
□	Does the SaaS vendor have a formal Security and Compliance program to ensure data protection for all data collected, stored or otherwise processed through their service?
□	Does the vendor only collect data from those who have given their consent by accepting the vendor's terms of service?
□	Does the vendor disclose the data residence for data collected, and does that residence meet data sovereignty and compliance regulations?
□	If an organization receives personal information that it has not solicited from an individual, will it collect only the data of customers who subscribe to their service?
□	Are details related to notifications for the collection of data covered in the vendor's Privacy Program, and are these details available on the vendor's website or via documentation provided by the vendor?
□	Does the vendor disclose the data residence for data collected, and does that residence meet data sovereignty and compliance regulations?
□	Has the vendor successfully completed the SSAE 16 SOC 2 audit certification process, a rigorous evaluation of repeatable operational and technical controls?
□	Does the vendor protect all data in transit with Secure Socket Layer (SSL) encryption?
□	Does the vendor protect data at rest with 256-bit AES object-level encryption—one of the strongest block ciphers available?
□	Does the vendor use systematic intrusion detection, including log analysis, file integrity checking, policy monitoring, rootkit detection, real-time alerting, and active response?
□	Does the vendor compartmentalize and limit access to the production environment, only granting access to named employees who have specific operational requirements?
□	If the vendor uses third party services, are those services ISO 27001 certified, have they completed multiple SAS-70 Type II audits, and do they publish a SOC 2 report under both the SSAE 16 and the ISAE 3402 professional standards?