

Testing true data sovereignty in practice

Could your provider technically access your data?

	Yes	No
Data location and legal access		
Where is your data stored – and is this clearly defined contractually?	<input type="checkbox"/>	<input type="checkbox"/>
Can you choose or control where your data resides?	<input type="checkbox"/>	<input type="checkbox"/>
Is the provider subject to legal obligations outside your jurisdiction that could allow access to your data?	<input type="checkbox"/>	<input type="checkbox"/>
Encryption and key control		
Is your data encrypted at every stage – before upload, during transfer, and in storage?	<input type="checkbox"/>	<input type="checkbox"/>
Is encryption applied on your side (client-side), before data reaches the cloud?	<input type="checkbox"/>	<input type="checkbox"/>
Do you (or your users) control the encryption keys – not the provider?	<input type="checkbox"/>	<input type="checkbox"/>
Does the solution provide end-to-end encryption with zero-knowledge protection, ensuring the provider cannot access keys or plaintext data?	<input type="checkbox"/>	<input type="checkbox"/>
If access were requested (legally or operationally), would it technically be possible?	<input type="checkbox"/>	<input type="checkbox"/>
Granular access and sharing controls		
Can you define exactly who can view, edit, download, or share your files – and for how long?	<input type="checkbox"/>	<input type="checkbox"/>
Can you assign clear roles and permissions for both internal teams and external stakeholders?	<input type="checkbox"/>	<input type="checkbox"/>
Can you enforce secure sharing with password protection, email verification, watermarking, download restrictions, and more?	<input type="checkbox"/>	<input type="checkbox"/>
Can you revoke access instantly if needed?	<input type="checkbox"/>	<input type="checkbox"/>
Can you centrally define and enforce policies across users and teams?	<input type="checkbox"/>	<input type="checkbox"/>
Visibility and auditability		
Can you track all file activities in real time – who accessed your data when and what actions were taken?	<input type="checkbox"/>	<input type="checkbox"/>
Are audit logs detailed, reliable, and exportable, supporting internal reviews and external audits?	<input type="checkbox"/>	<input type="checkbox"/>
Can you easily identify and remove outdated or unnecessary access rights?	<input type="checkbox"/>	<input type="checkbox"/>
Can you track and restore previous versions of files?	<input type="checkbox"/>	<input type="checkbox"/>