RampedUp
GLOBAL CONTACT DATA SOLUTIONS

Vendor Data Security Assessment

Vendor name: _____

Service provided: _____

Completed by / email: _____

Date: _____

RampedUp Data accessed or stored: _____

#	Security question	Response	Brief explanation, if needed
1	Have you assigned someone responsibility for data security and provided a security contact? Please provide that person's name and contact details.		
2	Do you have written security guidelines appropriate to your business and services? Please share your Information Security policy and any other Data Security documentation as an attachment.		
3	Do you collect and access only the RampedUp Data needed to provide the agreed service?		
4	Do you use RampedUp Data only for agreed purposes, with permission required for other uses, including AI model training?		
5	Does each person accessing RampedUp Data use their own device? If so how do you monitor our and protect the device as a policy?		
6	Do you limit access to people who need it for their work and review access periodically?		
7	Do you promptly remove access when someone leaves or no longer needs it? Explain your off-boarding process,		
8	Do you require multifactor authentication for administrator accounts and remote access to systems holding RampedUp Data?		

#	Security question	Response	Brief explanation, if needed
9	Do you use strong passwords and protect passwords, API keys, and other credentials from exposure? Please share your password policy.		
10	Is RampedUp Data encrypted when sent over the internet? If so, explain the process.		
11	Is stored RampedUp Data encrypted, including backups where applicable?		
12	Are computers used to access RampedUp Data protected by screen locks, disk encryption, and appropriate malware protection?		
13	Do you keep systems and software updated and prioritize fixes for serious security issues? Will you share your latest penetration testing if asked?		
14	Do you check for security weaknesses using methods appropriate to your service, such as vulnerability scans or security reviews?		
15	How do you protect RampedUp Data from unauthorized access?		
16	Do you record important access and administrative activity and review signs of suspicious activity?		
17	Do employees and contractors receive basic security guidance, including how to recognize phishing and report concerns? Explain,		
18	Are people with access to RampedUp Data subject to confidentiality obligations and background checks?		
19	Do you identify third parties that handle RampedUp Data and require appropriate security protections from them? List your sub-processors.		
20	Can you identify the countries where RampedUp Data is stored or accessed and communicate material changes?		
21	Where you are responsible for preserving RampedUp Data, do you maintain backups, test recovery, and have a basic disruption plan? Please share the DRP.		
22	Do you have a process to handle security incidents and notify us promptly of incidents affecting RampedUp Data? Explain the notification process		
23	Can you return or securely delete RampedUp Data when requested or when the service ends, with any retention exceptions and backup deletion periods explained?		

Vendor confirmation

To the best of my knowledge, these answers accurately describe the safeguards used for the service being assessed.

Name / title: _____ **Date:** _____

Internal review — completed by RampedUp

Decision: ☐ Approved ☐ Approved with follow-up ☐ Further review required

Open issues, agreed actions, owner, and target date:

Reviewer / date: _____

Review guidance: Assess gaps based on the sensitivity of the data and the access the vendor receives. A No or Partial answer does not automatically disqualify a vendor. Request supporting documents only where needed to resolve a material concern. Repeat the review annually for vendors with sensitive data or significant access, and when the service or data use materially changes.