



VENDOR SECURITY CHECKLIST


How to Vet a Call Center Partner for Data Protection?

Before signing with a contact center outsourcing provider, use this checklist to assess their commitment to security, privacy compliance, and data protection.

	1. LEGAL & REGULATORY COMPLIANCE	SCORE (/10)
1	Can the vendor comply with major data privacy laws (e.g., GDPR, CCPA, HIPAA)?	
2	Can they provide documentation of recent compliance audits or certifications?	
3	Is a Data Processing Agreement (DPA) included in the contract?	
4	Are subcontractors also compliant with these regulations?	
SCORE (/40)		




Under GDPR, your company is still liable even if a vendor causes a breach.

	2. EMPLOYEE ACCESS & TRAINING	SCORE (/10)
5	Do they enforce Role-Based Access Control (RBAC)?	
6	Are staff trained in data-handling protocols and phishing/social engineering awareness?	
7	Are regular background checks conducted for employees with data access?	
8	Do they run ongoing security training or simulated attacks (e.g., phishing tests)?	
SCORE (/40)		



Human error causes over 50% of data breaches. Training is your first defense.

	3. TECHNICAL SAFEGUARDS	SCORE (/10)
9	Is data encrypted at rest and in transit (e.g., AES-256, SFTP)?	
10	Do they use VPNs and/or Zero-Trust Architecture for remote agents?	
11	Are systems protected by firewalls, intrusion detection systems, and endpoint security?	
12	Is multi-factor authentication (MFA) required for system access?	
SCORE (/40)		



Encryption helps protect data even if intercepted during a transfer.

	4. MONITORING & INCIDENT RESPONSE	SCORE (/10)
13	Do they monitor system activity 24/7 with real-time alerts for anomalies ?	
14	Can they provide a clear data breach response plan ?	
15	Is there a defined escalation process for suspected security incidents?	
16	Have they had any prior breaches ? If so, how were they handled?	
		SCORE (/40)




A swift response to a breach can mitigate the risk of a PR disaster.

	5. AUDITS & REPORTING	SCORE (/10)
17	Do they conduct regular internal or third-party security audits ?	
18	Can they provide audit logs and compliance reports on request?	
19	Are KPIs related to data security part of the monthly performance reports?	
		SCORE (/30)



Regular audits help identify outdated protocols and minimize risk exposure.

	6. CONTRACTUAL GUARANTEES	SCORE (/10)
20	Is there a Service Level Agreement (SLA) with defined data protection metrics?	
21	Are penalties or liabilities defined in case of a breach?	
22	Are responsibilities split between data controller (you) and data processor (vendor)?	
23	Is there a termination clause with data destruction guarantees?	
		SCORE (/40)



Contracts should clearly state who is accountable for what.

How to Use This Checklist to Evaluate Your Vendor?

Assign a score from 0 to 10 for each checklist item based on how confidently your vendor meets the requirement.

- 10 = Fully meets the requirement
- 5 = Partially meets or unclear evidence
- 0 = Does not meet the requirement

There are 23 questions in total, so the maximum score is 230.

✓ Final Score Calculation:

1. Add up your total score (Maximum: 230).
2. Divide your score by 230.
3. Multiply the result by 100 to get your **Security Readiness Score (%)**.

🚩 Minimum Security Threshold: 75%

If your vendor's Security Readiness Score is below 75%, they may pose a significant data protection risk. In this case, you should either:

- Reassess their capabilities and improvement plan
- Or consider alternative providers with stronger security practices