Customer Data Protection Readiness Checklist

Score each item:

- Yes = 2 points
- Partially = 1 point
- No = 0 points

Data Visibility & Mapping

☐ We know all major locations where customer data currently exists across the business.
☐ We understand where unofficial customer copies commonly get created.
☐ We have reviewed customer data movement department by department.

Access & Accounts

☐ Former employee accounts are removed promptly from customer-facing systems.
☐ We use multifactor authentication on key customer data platforms.
☐ Shared generic logins are limited or eliminated where possible.
☐ We periodically review who can access customer records.

File Handling & Sharing

☐ Customer files are stored in standardized approved locations.
☐ Staff are discouraged from uncontrolled desktop/local downloads.
☐ “Anyone with link” file sharing is restricted for customer documents.
☐ Sensitive customer exports are not routinely emailed around the business.

Staff Behaviour & Training

☐ Employees understand the most common real-world customer data mistakes.
☐ Staff receive short practical customer handling guidance—not just generic cyber

lectures.
☐ Leadership models the same customer data discipline expected from staff.

Communication Security

☐ Customer identity verification is part of support/account-change workflows.
☐ We have boundaries on what customer information should not be sent through informal messaging apps.
☐ Staff are trained to check recipients carefully before sending attachments.

SaaS & Cloud Governance

☐ We review old SaaS users, permissions, and integrations periodically.
☐ Customer CRM exports are treated as exceptions rather than routine habits.
☐ We understand which cloud tools hold customer information.

Incident Readiness

☐ We have a simple first-response process for customer data exposure.
☐ We know who internally would coordinate containment.
☐ We can quickly identify which customers would be affected by a platform incident.

Long-Term Culture

☐ Customer data protection is treated as part of operational professionalism.
☐ We perform periodic cleanup of stale customer records and obsolete files.

SCORING RESULTS

38–48 Points — STRONG MATURITY

Your business has a healthy balance of customer data control, operational speed, and practical cybersecurity discipline.

20–37 Points — MODERATE EXPOSURE

You have some protective systems in place, but workflow inconsistencies still create avoidable customer trust and breach risks.

0–19 Points — HIGH VULNERABILITY

Customer data handling remains largely informal, fragmented