Privacy By Design Readiness Audit Checklist

Score each item:

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

Early Planning Discipline

☐ We map data categories before deploying new websites, apps, or workflows.
☐ We ask what information is truly necessary before adding form fields.
☐ We evaluate privacy impact during system planning — not after launch.

Access Control Structure

☐ New systems are built with role-based access rather than broad default visibility.
☐ Shared generic admin accounts are minimised.
☐ Contractor and temporary user access has expiration logic.

Vendor & Integration Governance

☐ We evaluate vendors based on data handling — not just convenience and price.
☐ We understand what customer data is duplicated across integrations.
☐ Inactive SaaS tools and old integrations are reviewed periodically.

Customer Workflow Design

☐ Customer information movement is mapped from inquiry to archive.
☐ Informal email/file hand-offs are minimised in customer workflows.
☐ Retention or deletion logic is considered during workflow setup.

Remote & Cloud Discipline

☐ Cloud collaboration environments have defined folder and sharing rules.
☐ Personal device use has explicit boundaries for business/customer data.
☐ Remote contractors do not receive indefinite broad access.

Documentation & Review

☐ We maintain practical records of systems, data owners, and vendor access.
☐ We perform scheduled privacy reviews of users, folders, and integrations.
☐ Our privacy policies are operationally usable, not just abstract statements.

Staff Alignment

☐ Employees know the approved pathways for storing and sharing information.
☐ Privacy expectations are tied to specific workflow tasks.
☐ Leadership follows the same privacy rules expected from staff.

Strategic Trust Positioning

☐ We view privacy maturity as part of customer confidence and brand professionalism.
☐ We can answer customer questions about data handling with clarity.

SCORING RESULTS

38–48 Points — STRONG MATURITY

Your organization demonstrates proactive privacy architecture, lower operational cyber debt, and strong long-term digital trust readiness.

20–37 Points — MODERATE EXPOSURE

Some intentional controls exist, but convenience-driven drift or reactive system growth still create avoidable privacy complexity.

0–19 Points — HIGH VULNERABILITY

Your digital systems appear largely convenience-built, making future cleanup, customer trust pressure, and data exposure significantly more likely.