



GDPR Readiness Audit Checklist

Score each item:

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

Website & Form Transparency

- Our website forms only collect information genuinely necessary for the service offered.
 - Users can easily understand why their information is being requested.
 - Our privacy notice reflects our real operational practices.
 - We know where website submissions are stored after form completion.
 - We periodically review lead magnets/download registrations for consent clarity.
-

Cookies, Tracking & Analytics

- We understand which analytics and marketing scripts are active on our website.
 - We have reviewed whether third-party tracking is excessive.
 - Cookie/consent mechanisms are not merely cosmetic.
 - We know which vendors receive visitor behavioural information.
-

CRM & Email Discipline

- We maintain subscriber and CRM databases with periodic cleanup.
 - We do not retain stale prospect information indefinitely without purpose.
 - Users can unsubscribe or manage communication preferences easily.
 - Internal CRM/customer record access is limited to relevant staff.
-

Internal Data Governance

- We know where employee records are stored across the business.
 - Staff/customer spreadsheets are not casually duplicated across unmanaged devices.
 - We have a designated person responsible for privacy oversight.
 - We review old, archived files and databases periodically.
-

Vendor & SaaS Oversight

- We know which third-party tools process customer or employee information.
 - We periodically remove unused plugins/accounts/vendors that still retain data.
 - We understand that vendor incidents still affect our business trust.
-

Incident Preparedness

- We have a basic documented process for handling data exposure incidents.
 - We know which internal systems would be reviewed first after a breach.
 - We can identify what customer information is stored in major business platforms.
-

Privacy Culture & Trust

- Staff understand that customer data handling is a trust issue, not just admin work.
 - We view privacy discipline as part of our brand professionalism.
-

SCORING RESULTS

40–48 Points — STRONG MATURITY

Your business demonstrates above-average privacy structure, operational awareness, and customer data discipline.

22–39 Points — MODERATE EXPOSURE

Your organization has partial safeguards in place, but several inconsistent processes still create preventable GDPR and trust risk.

0–21 Points — HIGH VULNERABILITY

Your current data handling appears informal, fragmented, or poorly documented, creating elevated privacy, reputational, and breach exposure.