GDPR Risk Register Report

Risk Description	Likelihood (1-5)	Impact (1-5)	Inherent Risk	Control(s)	Residual Risk	Treatment Plan
Non-compliance with lawful, fair, and transparent processing (Art. 5)	3	5	High	Privacy Policy, Consent Management System	Medium	Quarterly privacy audits, consent reviews
Incomplete records of processing activities (Art. 30)	2	4	Medium	Records of Processing Register (RoPA)	Low	Annual RoPA updates and audits
Weak technical & organizational measures (Art. 32)	4	5	High	Encryption, Access Controls, DRP	Medium	Quarterly DR tests, regular security reviews
Delayed or missed breach notification to authority (Art. 33)	3	5	High	Incident Response Plan, Breach Notification SOP	Medium	Tabletop breach simulations, IR updates
Failure to honor data subject rights (Art. 15-22)	3	4	Medium	DSAR process, DPO oversight	Medium	Employee training, quarterly DSAR reviews
Invalid consent management (Art. 7)	4	4	High	Consent forms, preference center	Medium	Annual consent review, transparency checks
Unsecured transmission of personal data (Art. 32)	3	5	High	TLS, VPN, encryption standards	Medium	Annual encryption audit, TLS certificate renewals
Lack of Data Protection Impact Assessments for high-risk processing (Art. 35)	2	4	Medium	DPIA procedures, risk assessments	Low	DPIA for all high-risk projects
Data retention beyond necessity (Art. 5)	3	3	Medium	Retention schedules, deletion policy	Low	Quarterly deletion reviews
Vendor risks or non-compliance with GDPR (Art. 28)	4	5	High	Vendor contracts, Data Processing Agreements (DPAs)	Medium	Vendor due diligence, yearly reviews