SAMPLE PRIVACY RISK REGISTER TEMPLATE

PRIVACY RISK REGISTER

Organization: [Your Organization Name]
PIMS Scope: [Brief scope description]
Version: [e.g., 1.0]
Date: [DD/MM/YYYY]
Prepared by: [Chief Privacy Officer / Privacy Team]
Approved by: [CEO / Board]
Next Review Date: [DD/MM/YYYY]

RISK ASSESSMENT CRITERIA

Likelihood Scale

Rating	Level	Description	Frequency
5	Almost Certain	Expected to occur in most circumstances	>80% probability; multiple times per year
4	Likely	Will probably occur	50-80% probability; at least once per year
3	Possible	Might occur at some time	20-50% probability; once every 1-3 years
2	Unlikely	Could occur but not expected	5-20% probability; once every 3-5 years
1	Rare	May occur only in exceptional circumstances	<5% probability; once every 5+ years

---

Impact Scale - PII Principals (Data Subjects)

Rating	Level	Impact on Individuals
5	Severe	Catastrophic harm: physical danger, severe financial loss (>€10,000), major psychological trauma, irreversible damage to reputation, identity theft with major consequences
4	Major	Serious harm: significant financial loss (€1,000-€10,000), significant distress or anxiety, discrimination, loss of employment, serious reputational damage
3	Moderate	Moderate harm: financial loss (€100-€1,000), considerable distress or embarrassment, damage to reputation, breach of sensitive information
2	Minor	Minor harm: minor financial loss (<€100), minor inconvenience or concern, limited embarrassment, temporary anxiety
1	Negligible	No significant impact: no noticeable harm, minor inconvenience easily rectified

---

Impact Scale - Organization

Rating	Level	Impact on Organization
5	Severe	>€1,000,000 financial impact; regulatory fine >€500,000; major reputational damage; loss of major customers; criminal prosecution; business closure risk
4	Major	€250,000-€1,000,000 impact; regulatory fine €100,000-€500,000; significant reputational damage; loss of customers; senior management accountability
3	Moderate	€50,000-€250,000 impact; regulatory fine €20,000-€100,000; moderate reputational damage; customer complaints; regulatory investigation
2	Minor	€10,000-€50,000 impact; regulatory warning; minor reputational impact; few customer complaints; internal investigation

1	Negligible	<€10,000 impact; no regulatory action; minimal or no reputational impact; no customer loss

---

Risk Matrix

	IMPACT				
LIKELIHOOD	**1-Negligible**	**2-Minor**	**3-Moderate**	**4-Major**	**5-Severe**
5-Almost Certain	**M** (5)	**H** (10)	**H** (15)	**C** (20)	**C** (25)
4-Likely	**M** (4)	**M** (8)	**H** (12)	**H** (16)	**C** (20)
3-Possible	**L** (3)	**M** (6)	**M** (9)	**H** (12)	**H** (15)
2-Unlikely	**L** (2)	**L** (4)	**M** (6)	**M** (8)	**H** (10)
1-Rare	**L** (1)	**L** (2)	**L** (3)	**M** (4)	**M** (5)

Risk Levels:

- **C = Critical (16-25):** Immediate action required; not acceptable
- **H = High (10-15):** Urgent action required within 30 days; not acceptable
- **M = Medium (5-9):** Action required within 90 days; may be accepted with management approval
- **L = Low (1-4):** Monitor; generally acceptable

PRIVACY RISK REGISTER

Risk ID	Risk Description	Category	Assets Affected	Threat Source	Existing Controls	L
PR-001	Unauthorized access to customer database by internal staff	Access Control	Customer PII database (names, emails, addresses, purchase history)	Malicious insider; Curious employee	Basic username/password; Access logs (not monitored)	3
PR-002	Personal data transmitted without encryption	Data in Transit	Customer data transmitted to payment processor	Network interception; Man-in-the-middle attack	HTTPS for web traffic	3
PR-003	No retention policy; customer data kept indefinitely	Data Retention	All customer databases	GDPR violation; Storage limitation principle breach	None	4
PR-004	Third-party marketing analytics provider has unrestricted access to customer profiles	Third-Party Processing	Customer behavioral data, preferences, demographics	Third-party data breach; Unauthorized use by vendor	Processor agreement (basic)	3
PR-005	Data subject access requests not responded to	Data Subject Rights	Customer data across all systems	Process failure; Resource constraints	Manual request handling; Email tracking	4

	within 30-day legal deadline					
PR-006	No Data Protection Impact Assessment conducted for AI recommendation engine	High-Risk Processing	Customer purchase history, browsing behavior	GDPR Article 35 non-compliance; Profiling without safeguards	None	4
PR-007	Customer consent mechanism uses pre-ticked boxes for marketing	Consent Compliance	Customer marketing preferences	GDPR Article 7 violation; Invalid consent	Pre-ticked checkbox consent form	5
PR-008	No privacy training for employees handling customer data	Awareness & Training	All customer PII	Human error; Unintentional disclosure	One-time onboarding session (outdated)	4
PR-009	Backup tapes stored offsite without encryption	Data Storage	Customer database backups	Physical theft; Lost media; Unauthorized access	Offsite storage facility (physical security only)	2
PR-010	Customer service staff can view full payment card details	Excessive Access	Payment card data (PCI scope)	Insider threat; Accidental disclosure; PCI DSS violation	Access controls (not restricted by role)	3

PR-011	Mobile app collects location data continuously without clear purpose or consent	Data Minimization	User location data (GPS coordinates)	Excessive collection; Purpose creep; Surveillance concerns	Generic privacy policy mention	4
PR-012	No incident response plan for privacy breaches	Incident Management	All PII	Delayed breach notification; Regulatory non-compliance; Inadequate response	General IT incident response (not privacy-specific)	3
PR-013	Cloud service provider (AWS) processes EU customer data; adequacy of data transfer mechanisms uncertain post-Schrems II	International Data Transfers	EU customer data stored in AWS (US company)	Schrems II invalidation; Inadequate transfer safeguards	Standard Contractual Clauses (SCCs)	3
PR-014	Employee monitoring (email, internet) conducted without transparent policy	Employee Privacy	Employee communications data	Lack of transparency; Employee rights violations; Trust erosion	Monitoring conducted; No formal policy	4

PR-015	Website uses non-essential cookies without prior consent	Cookie Compliance	Website visitor data (analytics, advertising cookies)	ePrivacy Directive violation; GDPR violation; Regulatory fine	Cookie banner (information only, no consent mechanism)	4
PR-016	No processor agreements with third-party vendors	Vendor Management	Customer data shared with 12 vendors	GDPR Article 28 violation; Vendor data breach; Lack of accountability	Vendor contracts (no privacy terms)	4
PR-017	Development and testing databases contain real customer data	Development Security	Customer PII in non-production environments	Unauthorized access; Lower security in dev/test; Data leakage	Production data copied to dev/test	3
PR-018	No privacy-by-design process for new products	Privacy by Design	All new product features	Privacy violations from poorly designed features; Retrofitting costs; Regulatory risks	Ad-hoc privacy reviews (inconsistent)	4

PR-019	Physical documents containing customer data not securely disposed	Physical Security	Printed customer records, reports	Dumpster diving; Physical theft; Unauthorized disclosure	General waste bins	2
PR-020	No regular privacy audits or compliance reviews	Compliance Monitoring	Entire PIMS	Undetected compliance gaps; Control failures; Regulatory violations	None	3

RISK TREATMENT SUMMARY

Risk Level	Count	% of Total	Action Required
Critical (16-25)	6	30%	Immediate action; must reduce within 30 days
High (10-15)	12	60%	Urgent action within 30-90 days
Medium (5-9)	1	5%	Action within 90 days or accept with approval
Low (1-4)	1	5%	Monitor; generally acceptable
TOTAL	20	100%	

RESIDUAL RISK SUMMARY

After all planned controls are implemented:

Residual Risk Level	Count	% of Total
Medium (5-9)	7	35%
Low (1-4)	13	65%

TOTAL	20	100%

All residual risks are within acceptable tolerance levels.

RISK TREATMENT PROGRESS

Status	Count	% Complete
Completed	0	0%
In Progress	8	40%
Planned	11	55%
Urgent (Start Immediately)	2	10%
On Hold	0	0%

KEY ACTIONS REQUIRED

Immediate Priority (Next 30 Days):

1. **PR-006:** Conduct DPIA for AI recommendation engine (CRITICAL)
2. **PR-011:** Implement purpose-specific location consent in mobile app (CRITICAL)
3. **PR-003:** Develop and approve data retention policy (CRITICAL)
4. **PR-016:** Execute processor agreements with all 12 vendors (CRITICAL)
5. **PR-005:** Complete request management system implementation (CRITICAL - 70% done)

High Priority (30-90 Days):

6. Complete all remaining HIGH risk treatments
7. Conduct privacy training for all employees
8. Implement privacy-by-design process
9. Execute incident response plan and conduct tabletop exercise

RISK OWNER APPROVALS

Risk Owner	Risks Owned	Approval Status	Residual Risk Acceptance	Date
CTO	PR-001, PR-002, PR-009, PR-010, PR-017	Approved	Accepted	[Date]
CPO	PR-003, PR-005, PR-012, PR-013, PR-020	Approved	Accepted	[Date]
VP Marketing	PR-004, PR-007, PR-015	Approved	Accepted	[Date]
Chief Product Officer	PR-006, PR-011, PR-018	Approved	Accepted	[Date]
CHRO	PR-008, PR-014	Approved	Accepted	[Date]
CFO	PR-010	Approved	Accepted	[Date]
COO	PR-016, PR-019	Approved	Accepted	[Date]

DOCUMENT APPROVAL

Role	Name	Signature	Date
Chief Privacy Officer	[Name]	_____	[Date]
Chief Executive Officer	[Name]	_____	[Date]
Board of Directors	[Name]	_____	[Date]

REVISION HISTORY

Version	Date	Changes Made	Approved By
1.0	[Date]	Initial risk register created	[CEO Name]

NOTES

Review Frequency: This risk register will be reviewed and updated:

- Monthly for risk treatment progress
- Quarterly for new risk identification
- Annually for comprehensive review
- Ad-hoc when significant changes occur (new systems, new processing, incidents, regulatory changes)

Escalation: Critical and High risks are reported to the Board quarterly. Any new Critical risks are escalated immediately.