**Data Protection Impact Assessment (DPIA) for Portfolio Website Contact Form**

1. **Purpose of the DPIA**

To assess privacy risks associated with the contact form on the Portfolio Co. website, which collects:

- Name & Surname

- Email Address

- Optional Message

- Anonymous submission preference

Legal Basis: Consent (GDPR Article 6(1)(a), POPIA Section 11).

1. **Data Flow & Processing Description**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Data Collected** | **Purpose** | **Storage Location** | **Retention Period** | **Shared with** |
| Name & Surname | Respond to inquiries | Encrypted database | 6 months | None |
| Email Address | Contact user | Encrypted database | 6 months | None |
| Message (Optional) | Clarify user request | Encrypted database | 6 months | None |
| Anonymous preference | Honor user privacy choice | Encrypted database | 6 months | None |

Data Flow:

1. User submits form -> Data stored in encrypted backend database.

2. Automated email confirmation sent to user.

3. Data deleted after 6 months (per Privacy Policy).

**3. Necessity**

Yes, Necessary?

- Name/email required to respond to inquiries.

- Anonymous option reduces data collection where possible.

Yes, Minimized?

- No unnecessary fields (e.g., phone number, address).

- Message field is optional.

Yes, Retention Justified?

- 6 months aligns with typical inquiry response windows.

1. **Identified Risks & Mitigations**

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk** | **Likelihood** | **Impact** | **Mitigation** |
| Unauthorized access (data breach) | Medium | High | Encryption, access controls, regular audits |
| Misuse of data (e.g., spam) | Low | Medium | No-sharing policy, anonymization option |
| Function creep | Low | Medium | Processing agreements, staff training |
| Non-compliance with deletion | Low | High | Clear Privacy Policy, opt-out process |

**5. Stakeholder Consultation**

- Internal: IT (security), Legal (Privacy compliance)

- External: None (low-risk)

- Data Subjects: Privacy Policy accessible; anonymous option provided

**6. Legal Compliance**

- GDPR: Consent obtained; right to erasure honored.

- POPIA: Section 18 notification requirements met (Privacy Policy explains processing).

- Special Categories: None collected.

**7. Approval & Monitoring**

Approval:

- [ ] DPO/Management: [Name, Date]

Monitoring Plan:

- Annual review of security measures.

- Update DPIA if form fields/processing changes.

**Conclusion**

The contact form poses low to medium risks, mitigated by encryption, minimal data collection, and user controls.