

# DATA PROTECTION IMPACT ASSESSMENT (DPIA) / PRIVACY IMPACT ASSESSMENT (PIA)

## Vendor Engagement Template

Available at [www.tpvrm.net/documents](http://www.tpvrm.net/documents) | The Future of Third-Party Risk Management & Data Privacy

A Data Protection Impact Assessment (DPIA) is required under GDPR Article 35 for processing activities that are likely to pose high risks to individuals' rights and freedoms. A Privacy Impact Assessment (PIA) has the same purpose under other relevant privacy laws. This template meets both requirements and should be started at the point when ITC completion and the scope assessment identify high-risk processing triggers.

This assessment must be reviewed and approved by the Privacy Officer or Data Protection Officer (DPO) before engaging the vendor. For EU personal data, the DPO's opinion must be documented.

## PART 1: ASSESSMENT IDENTIFICATION

|                                    |  |
|------------------------------------|--|
| Assessment Reference Number        |  |
| Vendor Name                        |  |
| Description of Processing Activity |  |
| Business Unit / Project            |  |
| Requestor                          |  |
| Privacy Officer / DPO Assigned     |  |
| Date Initiated                     |  |
| Target Completion Date             |  |
| Assessment Status                  |  |

## PART 2: TRIGGER ANALYSIS

A DPIA is required before processing that is "likely to result in a high risk to the rights and freedoms of natural persons" (GDPR Art. 35). Identify below which triggers apply to this engagement.

| Apply ?                                                     | DPIA/PIA Trigger                                                                                                                    | Notes |
|-------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|-------|
| <input type="checkbox"/> Yes<br><input type="checkbox"/> No | Systematic and extensive profiling or automated decision-making producing legal or similarly significant effects                    |       |
| <input type="checkbox"/> Yes<br><input type="checkbox"/> No | Large-scale processing of special categories of data (health, biometric, genetic, religious beliefs, racial or ethnic origin, etc.) |       |

| Apply ?                                                     | DPIA/PIA Trigger                                                                                             | Notes |
|-------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|-------|
| <input type="checkbox"/> Yes<br><input type="checkbox"/> No | Large-scale monitoring of publicly accessible areas (CCTV, geolocation, etc.)                                |       |
| <input type="checkbox"/> Yes<br><input type="checkbox"/> No | Processing of personal data of vulnerable populations (children, elderly, patients, employees)               |       |
| <input type="checkbox"/> Yes<br><input type="checkbox"/> No | Systematic cross-referencing or combining datasets beyond reasonable data subject expectations               |       |
| <input type="checkbox"/> Yes<br><input type="checkbox"/> No | Processing involving innovative technologies (AI, machine learning, biometrics, IoT)                         |       |
| <input type="checkbox"/> Yes<br><input type="checkbox"/> No | Transfer of personal data to a country without an EU adequacy decision and no alternative transfer mechanism |       |
| <input type="checkbox"/> Yes<br><input type="checkbox"/> No | Processing that prevents data subjects from exercising their rights or using a service or contract           |       |
| <input type="checkbox"/> Yes<br><input type="checkbox"/> No | Processing of personal data of 100,000 or more data subjects (large scale)                                   |       |

|                           |                                                                                                                                                            |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>DPIA/PIA Required?</b> | <input type="checkbox"/> Yes - Complete Parts 3-7 <input type="checkbox"/> No - Document rationale below <input type="checkbox"/> Consult DPO for decision |
| <b>Rationale (if No)</b>  |                                                                                                                                                            |

## PART 3: PROCESSING DESCRIPTION

### 3A. Processing Activity Description

|                                                                  |  |
|------------------------------------------------------------------|--|
| <b>Purpose of Processing</b>                                     |  |
| <b>Legal Basis for Processing (GDPR Art. 6)</b>                  |  |
| <b>Special Category Legal Basis (GDPR Art. 9, if applicable)</b> |  |
| <b>Categories of Personal Data Processed</b>                     |  |
| <b>Categories of Data Subjects</b>                               |  |
| <b>Estimated Number of Data Subjects</b>                         |  |
| <b>Data Retention Period</b>                                     |  |
| <b>Processing Location(s) /</b>                                  |  |

|           |  |
|-----------|--|
| Countries |  |
|-----------|--|

### 3B. Data Flow Description

Explain how personal data moves through the vendor engagement process, including collection, transfer, storage, processing, and deletion stages.

|                                                            |  |
|------------------------------------------------------------|--|
| Source of Personal Data                                    |  |
| How Data is Transferred to Vendor (mechanism and security) |  |
| Processing Activities Performed by Vendor                  |  |
| Subprocessors / Data Shared With                           |  |
| How Data is Returned / Destroyed at End                    |  |

## PART 4: NECESSITY AND PROPORTIONALITY

Evaluate whether the processing is necessary and proportionate to the purposes identified.

| Assessment Question                                                                                                          | Response |
|------------------------------------------------------------------------------------------------------------------------------|----------|
| Is the processing necessary to achieve the stated purpose? Could the purpose be achieved with less or no personal data?      |          |
| Is the processing limited to what is adequate, relevant, and necessary (data minimization)?                                  |          |
| Is the data retention period proportionate to the processing purpose? What happens to the data after it is no longer needed? |          |
| Are data subjects informed about the processing in a clear and accessible way (transparency)?                                |          |
| Are data subject rights (access, erasure, portability, objection) operable in this processing context?                       |          |
| Is there a legitimate basis for the processing under applicable law (GDPR                                                    |          |

| Assessment Question   | Response |
|-----------------------|----------|
| Art. 6, HIPAA, etc.)? |          |

## PART 5: RISK ASSESSMENT

For each risk area, evaluate the likelihood of occurrence (High / Medium / Low), the impact severity on data subjects if it occurs (High / Medium / Low), and identify mitigation measures. After implementing mitigation, evaluate the remaining risk level.

| Risk Area                                      | Risk Description                                                                                                                  | Likelihood | Severity | Inherent Risk | Mitigation Measures                                                                                                              | Residual Risk |
|------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|------------|----------|---------------|----------------------------------------------------------------------------------------------------------------------------------|---------------|
| <b>Unauthorized Access</b>                     | Vendor or third party gains unauthorized access to personal data. Risk increases with privileged access and poor access controls. | Medium     | High     | High          | MFA, least-privilege access, access logging, regular access reviews. Audit right in contract.                                    | Medium        |
| <b>Data Breach</b>                             | Personal data exposed through security incident at vendor. Ransomware, exfiltration, or unintended disclosure.                    | Medium     | High     | High          | Encryption at rest/transit, incident notification SLA, vendor SOC 2 certification, penetration testing requirement.              | Low           |
| <b>Excessive Collection</b>                    | Vendor collects more personal data than necessary for the stated purpose.                                                         | Low        | Medium   | Medium        | Data minimization clause in DPA. ITC scope assessment limits data types. Periodic review of data collected.                      | Low           |
| <b>Unlawful Subprocessing</b>                  | Vendor shares personal data with subprocessors without authorization or without equivalent protections.                           | Low        | High     | Medium        | DPA requires prior approval or advance notice for subprocessors. Subprocessor list maintained and monitored.                     | Low           |
| <b>Cross-Border Transfer Without Mechanism</b> | Personal data transferred to countries without adequate protection and no valid transfer mechanism (SCCs, etc.).                  | Low        | High     | Medium        | Data residency clause in contract. Transfer mechanism documented (SCCs). Data location identified in DPA.                        | Low           |
| <b>Failure to Honor Data Subject Rights</b>    | Vendor delays or prevents organization from fulfilling data subject access, erasure, or portability requests.                     | Low        | Medium   | Medium        | DPA includes data subject rights assistance obligation with defined timelines. Tested in onboarding.                             | Low           |
| <b>Retention Beyond Purpose</b>                | Vendor retains personal data beyond the agreed period or after contract termination.                                              | Medium     | Medium   | Medium        | DPA specifies deletion/return obligation and timeline. Certificate of destruction required. Offboarding checklist.               | Low           |
| <b>AI-Related Risks</b>                        | Vendor uses AI to process personal data in ways not disclosed, or AI-generated profiles used for consequential decisions.         | Medium     | High     | High          | AI governance provisions in contract. Prohibition on training data use. Model transparency requirements. Human oversight clause. | Medium        |

## Overall Risk Assessment

|                                    |                                                                                                                                                                                                           |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Overall Residual Risk Level</b> | <input type="checkbox"/> High - Prior consultation with DPA required (GDPR Art. 36) <input type="checkbox"/> Medium - DPO review required <input type="checkbox"/> Low - Proceed with documented controls |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## PART 6: MEASURES AND APPROVALS

### 6A. Measures to Address Risks

List all technical and organizational measures agreed upon to lower identified risks to acceptable levels.

| Measure | Risk(s) Addressed | Owner | Target Date |
|---------|-------------------|-------|-------------|
|         |                   |       |             |
|         |                   |       |             |
|         |                   |       |             |
|         |                   |       |             |
|         |                   |       |             |

### 6B. DPO Opinion (Required for EU Personal Data - GDPR Art. 35(2))

|                             |                                                                                                                                                                                      |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>DPO Name / Title</b>     |                                                                                                                                                                                      |
| <b>DPO Opinion Summary</b>  |                                                                                                                                                                                      |
| <b>DPO Recommendation</b>   | <input type="checkbox"/> Approve Processing <input type="checkbox"/> Approve with Conditions <input type="checkbox"/> Reject <input type="checkbox"/> Refer to Supervisory Authority |
| <b>DPO Signature / Date</b> |                                                                                                                                                                                      |

### 6C. Final Approval

|                                                    |                                                                                                                                                    |
|----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Privacy Officer / Controller Representative</b> |                                                                                                                                                    |
| <b>Approval Decision</b>                           | <input type="checkbox"/> Approved <input type="checkbox"/> Approved with Conditions <input type="checkbox"/> Rejected - Processing may not proceed |
| <b>Date of Decision</b>                            |                                                                                                                                                    |
| <b>Conditions (if applicable)</b>                  |                                                                                                                                                    |
| <b>Next Review Date</b>                            |                                                                                                                                                    |