

Vendor DPIA

1. **General Information - Emburse**
 - 1.1. DPIA revision date
 - 1.2. Vendor name, Vendor headquarter address, and URL
 - 1.3. Is this a new Vendor
 - 1.4. Name of the Vendor business representative
 - 1.5. Name of Emburse business representative
 - 1.6. List executed Processing agreements (MSA, DPA, etc.) and the date of execution
 - 1.7. Attach the executed agreements
 - 1.8. Describe the services performed by this Vendor
 - 1.9. Describe the scope of the Processing
 - 1.10. Identify the level of difficulty to replace the Vendor
 - 1.11. How essential to core company operations is the Vendor and the services they provide?
 - 1.12. Identify impact level (financial, operational, service standards, or other) that disruption of service provided by Vendor or termination of contract would cause
 - 1.13. Approximate amount of Personal Data being Processed
2. **Processing**
 - 2.1. Source of the data - **Emburse**
 - 2.2. Data collection mechanism - **Emburse**
 - 2.3. Data use (explain all possible uses) - **Emburse**
 - 2.4. List all the countries where Personal Data will be Processed - **Vendor**
 - 2.5. List all the Countries where Personal Data will be accessed - **Vendor**
 - 2.6. List all the countries where Personal Data will be stored - **Vendor**
 - 2.7. Does the Vendor retain Emburse and/or Personal Data (including PII or PHI) on their information systems? - **Vendor**
 - 2.8. Explain data deletion procedures (How will it be deleted? When will Personal/Emburse Data be deleted) - **Vendor**
 - 2.9. Explain Personal Data retention procedures (Does Vendor retain any copies of the data? If so, for what purpose?) - **Vendor**
 - 2.10. Applicable data maps (Attach copy) - **Vendor**
3. **Data Type - Emburse**
 - 3.1. List all the categories of Personal Data being Processed(e.g., name, DOB, address, etc.)

- 3.2. List all GDPR special Personal Data categories being Processed (e.g., gender, political affiliation, etc.)
 - 3.3. Does the Personal Data being Processed include Emburse Employee Personal Data
4. **Purpose**
 - 4.1. Intended purpose of the Processing (What does the team intend to accomplish when Processing the Personal Data?) - **Emburse**
 - 4.2. Benefits of the Processing - **Emburse**
 - 4.3. Will the Personal Data be used for anything other than the intended purpose? - **Vendor**
 - 4.4. Is Vendor selling Personal Data (as defined by CCPA)? - **Vendor**
 - 4.5. Is Vendor considered a Personal Data Broker (as defined by CCPA)? - **Vendor**
 - 4.6. Identify the level of sensitivity of the Personal Data being exchanged between Emburse and the Vendor - **Emburse**
5. **Legitimate basis for Personal Data Processing** (Check all applicable)
 - 5.1. Consent
 - 5.2. Performance of a contract
 - 5.3. Legitimate interest
 - 5.4. Legal requirement
 - 5.5. Public interest
6. **Data Subject Rights - Vendor**
 - 6.1. Correction
 - 6.2. Deletion
 - 6.3. Compliance with Other GDPR and CCPA Rights
7. **Subprocessors - Vendor**
 - 7.1. List All Subprocessors
 - 7.2. Explain the Service Provided by Each Subprocessor
 - 7.3. Explain Why the Subprocessor Is Needed
 - 7.4. List All Information Shared by Subprocessors to Additional Vendors
 - 7.5. List All Systems that Require Integrations (Marketo or Salesforce)?
 - 7.6. List All Data Shared Externally
 - 7.7. Is the Personal Data being used for any internal purpose(s)? (e.g., business purposes, service improvement, etc.)
8. **Sensitive Data Processing - Vendor**

- 8.1. Does the Processing involve profiling?
- 8.2. Does the Processing require automated decision making?
- 8.3. Can the Processing be used to observe, monitor, or influence Data Subjects?

9. **Security - Vendor**

- 9.1. How is access controlled?
- 9.2. What procedures are in place to determine who may access Personal Data?
- 9.3. Describe the Vendor's Privacy Training Program (frequency, content, etc.). Please provide supporting documentation
- 9.4. Explain the Vendor's auditing procedures
- 9.5. Data Protection in Transit
- 9.6. Data Protection at Rest
- 9.7. List technical measures in place to prevent excessive or unnecessary Processing
- 9.8. SOC1, SOC2, PCI or ISO 27001? Please provide the list and documentation for all the available certifications
- 9.9. Has Vendor had a confirmed Personal Data Breach in the last 2 years?

10. **Regulated Fields - Vendor**

- 10.1. Does the Vendor, Vendor Parent Company, or Vendor's Subprocessors fall under any of the following definitions under 50 U.S.C. Section 18881(b)(4)
- 10.2. Telecommunications Carrier
- 10.3. Electronic Communications Service
- 10.4. Remote Computing Service
- 10.5. Does Vendor, Vendor Parent Company, or Vendor's Subprocessors cooperate in any respect with US Authorities conducting surveillance of communications under:
- 10.6. EO 12333
- 10.7. Foreign Intelligence Surveillance Act (FISA)
- 10.8. Section 702 of FISA
- 10.9. Section 215 of the USA Patriot Act