Third Party Vendor-Privacy Assessment

Version 9

REZOLVE.ai

Document Information

Name of the document	Third Party Vendor-Privacy Assessment
Release date	27-Dec-18
Owned by	Mayank Baghel
Governed by	Mr.Udaya Bhaskar Reddy

Revision History

Version No	Version Date	Details of Change
1	5-Dec-2018	Initially Drafted
2	10-Dec-2018	Final
3	15-Dec-2020	Reviewed and no change
4	02-Dec-2021	Reviewed and no change
5	04-Mar-2022	Updated Document Information
6	02-Mar-2023	Reviewed and no change
7	26-Sep-2024	Updated Document Information
8	23-Mar-2025	Updated the document details as per migration from ISO 27001:2013 to ISO27001:2022
9	29-May-2026	Reviewed and no change

Reviewer and Approver

Name	Title	Comments	Date
Mr.Udaya Bhaskar Reddy	Co-Founder & CTO	Approved	04-June-2026

Table of Contents

1. Purpose and Scope

GDPR requirement
In GDPR terms, a "data controller" must perform due diligence on the "data processors" to whom it outsources the processing of personal Data. The key issue is that Data Controller assume joint responsibility should one of the Third Parties be breached. Failure of Company's Third-Party data processor to adhere to GDPR requirements means financial penalties.
Third parties, which could range from marketing agencies, law firms, to individual contractors such as software programmers, and all must also comply with the GDPR if they are involved in any way with the collection or processing of personal data for employees, customers or contacts.

Purpose
This document contains guidelines that should be met to maintain the security of Company information systems and data when the Company enters into any arrangement with a third party.

Scope
This document should be understood by all employees who seek to source a service from a third party that would give them direct access to Company data. This may involve the service run on systems outside of the Company in the cloud or where support agreements give the third-party access to Company systems.

- Whenever a controller uses a processor it needs to have a written contract in place.
- The contract is important so that both parties understand their responsibilities and liabilities.

Definitions

- **Third Party** is any entity providing services to Company but not under direct business control of the Company. In this document, the term "third party" refers to any person or entity other than the Company or its clients that has entered into a contract, a master agreement or a statement of work (SOW). Throughout this document, the term "Third Party" encompasses the, but is not limited to, the following:
    - Business Partners / Business Associates
    - Contract employees (Sub-Contractors)
    - Corp-IT service providers
    - Support Services (Security companies, Housekeeping, catering etc.)
    - Vendors/suppliers of products or services
    - Marketing partners
    - Freelancers

Key vendors are those third parties who are involved in providing the service(s) that Company provide to its clients. These third parties will have a direct impact on the Company's controls related to confidentiality, integrity and availability of information.

Risk management area is responsible for performing initial and annual third-party risk assessments and periodic monitoring activity.
Third party risk management encompasses vendor risk management but is more broadly focused on gaining an understanding of organizational risks and understanding which of those risks may be either positively or negatively affected by third parties.

1. Policy Standards

Principles

An effective risk management process throughout the lifecycle of the relationship includes:

- Proper due diligence in selecting a third party through a formal selection process.
- Written contracts that outline the rights and responsibilities of all parties.
- Ongoing monitoring of the third party's activities and performance.
- Contingency plans for terminating the relationship in an effective manner.
- Clear roles and responsibilities for overseeing and managing the relationship and risk management process.
- Documentation and reporting that facilitates oversight, accountability, monitoring, and risk management.

Policy Requirements
Following requirements are applicable to all third-party providers including vendors.

- GDPR requires that all downstream processors, vendors who handle personal data are required to have an enforceable and signed agreement/contract with the Company.
- All user teams should follow the third-party selection process before being appointed.
- All third party should sign agreements before services are delivered. Agreements will follow Company's policies and should include confidentiality and non-disclosure terms.
- There will be an annually review done for all third parties.
- Third party's onsite employees should comply with all Company's policies and procedures.
- Third party's employees who are on Company's site should be background screened by the vendor and evidence provided to the Company. Background screening should meet Company's policies.

Company as a Controller

- Controllers must only appoint processors who can provide ‘sufficient guarantees' that the requirements of the GDPR will be met and the rights of data subjects protected.
- The Company is a Controller for personal data of its direct clients. Any sub processor engaged to handle this data needs to be subject to this policy.

Company as a Processor

- The Company as the processor must only act on the documented instructions of a controller. The Company is a data processor for personal data processed.
- Where the Company as a processor engages another sub-processor, the same data protection obligations as set out in the contract or other legal act between the controller and the company shall be imposed on that other processor by way of a contract in particular providing sufficient guarantees to implement appropriate technical and organisational measures.
- Where that other sub-processor fails to fulfil its data protection obligations, the company shall remain fully liable to the controller for the performance of that other processor's obligations.

GDPR Compliant Contracts
Whether the Company is a Controller and engages a Processor, or the Company is a Processor and engages a sub-processor, the contract requirements are more or less the same. The following outlines the mandatory clauses of the contract:

- The subject matter and duration of the processing.
- The nature and purpose of the processing.
- The type of personal data and categories of data subject.
- The obligations and rights of the controller.
- The processor must only act on the written instructions of the controller.
- Persons authorised to process the personal data have committed themselves to confidentiality (NDA, background screening etc.).
- The processor must take appropriate measures to ensure the security of processing.
- The processor must only engage a sub-processor with the prior consent of the data controller and a written contract.
- The processor must assist the controller in allowing data subjects to exercise their rights under the GDPR
- The processor must assist the controller in meeting its GDPR obligations.

- The processor must delete or return all personal data to the controller as requested at the end of the contract; and
- The Company retains the right to audit third party premises and security practices to ensure their compliance with contract terms and the company policies. All related third-party information, security policies must be made available to the Company.
- Contracts shall document third party security roles and responsibilities.
- Contract shall identify local, legal/regulatory requirements including privacy and data protection.
- Contracts should require that third party reports all security breaches, including confidentiality and privacy violations, in a timely manner to allow for appropriate breach containment and eradication.
- Definition, reporting and monitoring of the third parties service performance levels must be agreed upon in the contract.

1.5.1 Standard Contract Clause
The GDPR allows for standard contractual clauses from the EU Commission or a supervisory authority to be used in contracts between controllers and processors. As and when these are available, the Company may decide to use those instead of internal contract formats.

Non-Disclosure Agreements (NDA)
The third party must adhere to an NDA prior to having access to any sensitive Company or client information. In some circumstances, the NDA may be signed before final approval of the contract.

Risk Assessment
The third-party services security must be evaluated as part of the vendor evaluation. Accordingly, a risk assessment may be conducted to assess the security of the third party's infrastructure, premises, policies, standards, and procedures in relation to its contracted functions (Out-sourcing included). The risk assessment may recommend appropriate security controls.
Following risk assessments will be done.

- Initial risk assessment - This risk assessment will be done at the beginning of the relationship. Risk management area will perform and validate this assessment. Risk assessment will follow templates given in Annexure. The initial risk assessment will be maintained by the user areas along with other third-party documents.
- Annual risk assessment - Annually the initial risk assessment will be reviewed for any changes in risks, emerging or new risks.

The risk assessments will consider following risks.

- Information Security & Privacy risk
- Physical security risk
- Operational risk
- Business continuity & resilience risk
- Reputational risk
- Compliance

1.7.1 Risk assessment format
Ensure that third parties are risk-scored according to assessments and other due diligence. For high-risk third parties, identify audit partners for the assessment of processes and to determine if on-site audits are required. Agree with your compliance team about the scope of remediation programs and ongoing monitoring requirements.
"Due Diligence Checklist" will be completed for all key vendors.

1. Third Party Selection and Monitoring
   Selection Process

Every third-party requirements may vary from user department to department. However, following generic process should be followed.

- Examining Business Requirements - The first and one of the most important steps in the vendor selection process is to examine and carefully analyze the business requirement. Ideally, user teams should be very clear on what services they intend to outsource to a third-party.
- Request for Proposal & Request for Quotation - After preparing the list of vendors that will be capable of providing the required services, the user team can then ask the service providers for a formal proposal. The proposal should contain all the details including scope, requirements, capability details, commercials, and the necessary terms and conditions.
- Vendor Selection - All the proposals are analyzed carefully. Following should be considered at the minimum.
    - Capability review (can third party meet the requirements). Operational capabilities will be assessed whether the third party is capable of meeting requirements.
    - GDPR Privacy Assessment
    - Evaluate vendors' awareness of GDPR. Request them to complete a short questionnaire on their GDPR preparedness.
    - Ensure that they have appropriate technical and organizational measures in place to comply.
    - Security requirements - For third parties that will impact security, confidentiality, or availability, a security assessment will be essential. This will be done by the Risk Management Team.
    - Financial assessment to determine financial ability to provide services. Commercial signoff from Finance.
- Negotiation and Contract signing - Finance will get involved in the negotiation stage. A negotiation committee may be set up consisting of domain experts and Finance/Legal. Once the vendor has been selected, the last important step is to draft the contract. The various risks and liabilities associated with signing a contract need to be examined thoroughly before the contract is signed. Finance delegation guidelines will be followed for getting approvals and contract signing.

Vendor Monitoring
Third party shall be monitored for compliance to security controls and service performance levels. Independent audit reports shall be produced where risk assessment justifies it.

- Performance Monitoring - Key third party's performance should be monitored on a regular basis. The user area will produce dashboard reports tracking actual SLs versus committed SLs.
- System Performance Monitoring - If vendor is providing systems related services then systems performance should be monitored using the following means:
    - Monitoring system dashboards, logs, notifications/alerts.
    - Monitoring service level agreements (SLAs), terms of agreement, warranties, and guarantees.
    - Reviewing and reconciling reports coming from vendor's systems.
    - Holding periodic discussions with the vendor organization.
    - Making regular site visits and completing site visit reports.
    - Testing controls at the sub-service organization via members of the Company's internal audit function.
    - Monitoring external communications.
- Risk Assessment - Risks related to third party's service delivery must be included in the Company's risk assessment.

1.2.1List of Customers and Vendors

To ensure that all third parties are engaged only after entering into a written contract along with appropriate Data Protection Addendum, the company shall maintain a list of Customer and Vendors as per "List of Contracts with Customer and Sub Processors"

NOTE - Next review cycle for this policy is **March-2027**. Management can review policy any time and can make changes depending on the situation.

***** All documents related to policies and procedures any reference to Actionable Science is as good as Rezolve.ai