REDCLOVER ADVISORS

# Third-Party Risk Management Guide

www.redcloveradvisors.com | info@redcloveradvisors.com

REDCLOVER ADVISORS

# A Step-By-Step Guide

Entrusting third-party vendors with your organization's personal data can significantly heighten your risk exposure. Security Magazine reports that a staggering 52% of data breaches are attributed to third parties.

Our guide offers a comprehensive solution for establishing a third-party assessment and management program, designed specifically to minimize these risks and promote compliance with privacy and data protection laws.

1

## PRIVACY AND SECURITY ASSESSMENT

Create a process to ensure the vendor can uphold your privacy and security obligations.

## SECURE TRANSFER METHOD

Determine how you will transfer or provide access to your personal data in a secure and privacy protective manner.

3


## DATA PROTECTION AGREEMENTS

Ensure your contracts meet your legal obligations and include limitations on vendors' use and sharing of the personal data you share with it.

2

## REGULAR MONITORING

Create a review process and determine an appropriate cadence for auditing a vendor's compliance with the contract.

4

## APPROPRIATE OFFBOARDING

Create a process for deletion, destruction, return, or removal of access to personal data at the end of the agreement.

5

**CAUTION!**

Under some privacy laws, you may be "selling" or "sharing" personal data if contracts with your vendors don't include restrictions on how they can use your personal data.



www.redcloveradvisors.com | info@redcloveradvisors.com

## 1 Privacy & Security Assessment

When bringing on a new vendor, it's important that you ensure they can uphold the privacy and security promises that your organization has made to customers, employees, and others.

### Some important areas to investigate include:

- What reputation does the company have and have they had any recent data breaches or security incidents?
- How much experience do they have in supporting the proposed processing?
- Do they have security certifications (e.g., ISO 27001, SOC2 Type 2)?
- What commitments do they make in their privacy notice?
- Does their internal privacy and security documentation look complete and compliant with applicable data privacy laws?
- Do they have an established data incident and breach response plan in place?
- Do they have the staff and resources available to protect your personal data to your standards?
- Where cross-border transfer is involved, have they self-certified to the Trans-Atlantic Data Privacy Framework or another data transfer mechanism?

## 2 Data Protection Agreements

Many privacy and data protection regulations mandate the inclusion of specific details in agreements that entail sharing personal data with a vendor, often referred to as a service provider or data processor.

### Key details to incorporate into your agreements with vendors include:

- The categories of information to be processed.
- The duration of the processing and location of the personal data.
- The obligation to process personal information only as instructed by you.
- The obligation to comply with applicable data protection laws.
- Their security obligations.
- Obligations around data breach including liability and notification.
- The requirement to notify you if they can no longer meet contractual obligations.
- Obligations around further sharing, such as using sub-processors.
- Their role in assisting you in compliance, particularly in honoring individual rights requests.
- Your right to monitor compliance with the contract.
- Instructions on the return or destruction of personal data at the end of the agreement.

## 3 Secure Transfer Mechanism

It is essential that you have a secure method to provide vendors access to the relevant personal data or to transfer the personal data to them. This will look different depending on the sensitivity of the personal data and the processing activity to be performed.

First and foremost, you want to make sure you're only giving the vendor the information necessary to do the work they're contracted to do.

**Then consider:**

- How can you redact datasets so vendors can only access the information necessary for the contract?
- What types of encryption are available?
- Can you provide access through a cloud solution under your control?
- What type of authentication makes sense with the level of risk?
- Can you require use of a VPN for access?
- What access controls are available at the user-level?
- What are your cross-border transfer obligations, if any?

## 4 Third-Party Vendor Monitoring

Your diligence doesn't stop once a vendor is selected and an appropriate contract is signed. It is important that you monitor vendors to ensure they are protecting your data and processing it as directed in the contract. A monitoring program may involve spot tests for security, reports on performance, compliance, security vulnerabilities, regular audits, and more.

Your right to monitor a vendor's compliance should be written into your contract and will largely depend on the categories of information you're sharing with them, and the type of processing involved

**Key details to incorporate into your agreements with vendors include:**

- What to include in your monitoring program.
- Metrics for measuring a vendor's technical security obligations.
- Metrics for measuring privacy practices.
- How often to audit a particular vendor.
- Whether you should use an independent auditor.
- What departments need to be included in an audit.
- What methods will you use to audit (document review, stakeholder interviews, review of publicly available information)..
- What roles will have responsibilities for vendor monitoring and documentation around roles and responsibilities.

## 5 Appropriate Offboarding

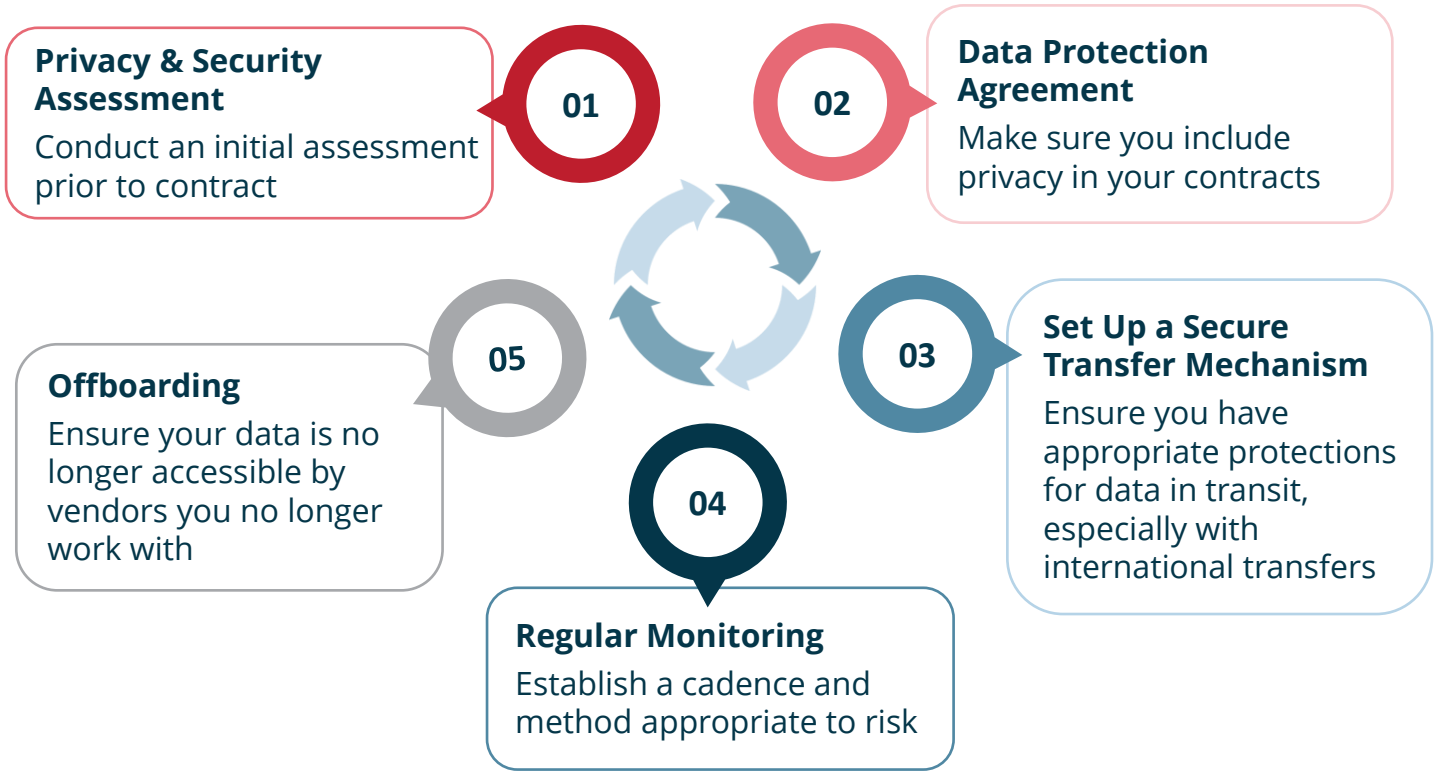
Much like data, vendors also have a lifecycle. And much like managing privacy obligations, managing your vendors and the data that they process needs to continue until they destroy or return your personal data to you.

It is important to consider the sunsetting of a relationship with a vendor at the outset of the relationship.

### In particular, you should consider:

- How you will ensure the vendor no longer has access to any systems or networks you have shared (e.g., physical space, devices, user accounts).
- What systems and processes may be impacted by the change.
- What internal roles and teams should be notified of the change.
- Whether you need to update your internal policies or processes or your external-facing privacy notice because of this change.
- How this change impacts your data mapping and/or records of processing activities.
- *And make sure to update your vendor inventory!*

### THIRD-PARTY VENDOR RISK MANAGEMENT CYCLE



REDCLOVER ADVISORS

# THIRD-PARTY RISK MANAGEMENT

## Set Yourself Up for Success

### Assessment Questionnaire

Work with your privacy and security teams to create a standard privacy and security questionnaire that you can easily send to new vendors. A combined assessment streamlines the process for you and for the vendor.

### Data Protection Agreements

Work with your legal team or outside counsel to create a standard data protection agreement that aligns with your practices. Even in circumstances where you sign the vendor's contract, it is a useful comparison tool to ensure the contract meets your needs.

### ASSESSMENT CADENCE

Look to your data classification policy and privacy impact assessment (See our Privacy Rights Roadmap: Business Guide to determine an appropriate cadence for privacy and security reviews based on the risks related to the personal data transferred and the processing activity.

### TRAINING

Training isn't just for employees that may interact with consumers, it's equally important for those responsible for onboarding and managing vendors. Appropriate, role-based training equips these individuals with the knowledge to effectively manage these relationships to safeguard personal data.

### CROSS-BORDER TRANSFER

Determine an appropriate mechanism to ensure appropriate protections in cross-border transfer of personal data. This will depend on the jurisdiction, so know your obligations before entering into contracts with vendors in other regions.