Fey | LLC Attorneys at Law

PRIVACY & INFORMATION GOVERNANCE SOLUTIONS

Third Party Vendor Risk Management Checklist

This checklist contains high-level considerations to help organizations manage the risk of Third Party Vendors with access to their data. This is not intended to be an exhaustive list; rather, it is intended to highlight key factors that we anticipate many organizations would want to contemplate when engaging Vendors to perform services that involve access to their data (*e.g.*, entering into a Software as a Service Agreement with a cloud service provider; outsourcing customer service functions involving personal data; deploying medical devices that will transmit data to a third party cloud server).

Determine Level of Due Diligence Required in Light of Type[s] of Personal Data to be Collected; Processing Activities; and Applicable Laws, Regulations, Policies, Procedures and Contracts

- ☐ Conduct internal assessment to evaluate the types of data that will be collected by the Vendor, including employee and customer personal data ("Personal Data"), and the scope and depth of processing activities the Vendor will be conducting.
- ☐ Analyze pertinent data privacy and protection laws and regulations, as well as any applicable policies, procedures and contracts (*e.g.*, customer contracts).
- ☐ Consider how the Vendor will collect Personal Data and whether and how the Vendor will share Personal Data with other third parties.
- ☐ Analyze the level of risk of harm to customers, employees, and to the organization if the security of data is compromised or if there is a data breach.
- ☐ Determine the level of due diligence that should be applied to Vendor selection and management based upon these factors.

Vet Vendor Candidates

- ☐ Consider business reputation and current financial condition of the potential Vendor.
- ☐ Analyze potential Vendor's experience implementing and supporting the proposed activity (including Personal Data handling).
- ☐ Search for publicly available information concerning security incidents/data breaches involving the potential Vendor.

- ☐ Review any other negative media coverage, as well as information concerning significant litigation or regulatory actions pending against the potential Vendor and publicized client complaints.

Confirm Vendor has an Acceptable Data Privacy and Security Program in Place

- ☐ Request and review pertinent Vendor documents pertaining to data privacy and information security issues and practices (*e.g.*, copies of security and privacy audit reports).
- ☐ Evaluate the Vendor's internal data privacy and information security policies, procedures, and processes.
- ☐ Assess the Vendor's downstream third party sharing practices.
- ☐ Determine the steps and processes the Vendor utilizes with respect to quality and accuracy of collected data, as well as access to and amendment of such data.
- ☐ Analyze the extent to which the Vendor allows on-site audits or currently engages any third party to provide verification of controls relating to security, availability, processing integrity, confidentiality, and privacy.
- ☐ Determine whether the Vendor has cyber-insurance.
- ☐ Ascertain the policies and procedures the Vendor has in place for management of security incidents and data breaches.
- ☐ Evaluate the Vendor's disaster recovery and business continuity planning.
- ☐ Request contact information for similarly situated Vendor customers, and contact them to obtain information concerning their experiences with the Vendor (*e.g.*, the Vendor's data privacy and information security practices).
- ☐ Document Vendor selection criteria and Vendor findings.

Negotiate Contract with Vendor

- ☐ Identify required terms (including clauses pertaining to data privacy and information security), and incorporate such terms into the Vendor contract.
- ☐ Identify prohibited terms (*e.g.*, unilateral indemnification clauses), and strike any such terms out of the Vendor contract.
- ☐ Negotiate as necessary.
- ☐ To streamline Vendor contracting processes moving forward, consider developing Checklists (*e.g.*, checklist of requisite and prohibited terms) and a template Vendor contract.

Implement Contract with Vendor

- ☐ Develop a process for ensuring that all affected employees are aware of obligations imposed by finalized contracts with Vendors.

Monitor Vendor Compliance

- ☐ Select monitoring approach.
- ☐ Conduct annual compliance monitoring, as well as monitoring compliance on an "as needed" basis.

Prepare for Potential Vendor Breach

- ☐ Confirm organization's Security Incident Response Procedures cover Vendor security incidents.
- ☐ Request and review Vendor's Security Incident Response Procedures.
- ☐ Include key Vendors in incident response planning and tabletop exercises.

If a Vendor Contract Must Be Terminated

- ☐ Prepare for termination, including reviewing contract provisions and deadlines, and compiling a list of all reasons supporting termination.
- ☐ Proceed with termination steps, including revoking Vendor access, ensuring Vendor return or disposal of data, and transitioning to new Vendor (if any).

If you have any questions concerning this Checklist or related issues, or if you would like assistance conducting a data privacy risk assessment in connection with a Third Party Vendor transaction; negotiating terms with a Vendor; developing a detailed, organization-specific checklist of required and prohibited terms for vendor contracts; or drafting and implementing policies and procedures to manage the vendor relationship from selection to termination, please contact: **Laura Clark Fey at (913) 948-6301 or lfey@feyllc.com.**

This Vendor Risk Management Checklist has been prepared by Fey LLC as an exemplar only and as a high-level overview of risk management considerations. This Vendor Risk Management Checklist is not intended as legal advice, and is also not intended to detail every risk management consideration that could be included in an analysis of a Vendor. Any entity seeking to engage a Vendor should analyze its own data privacy and information security practices, as well as any internal records and information governance, data privacy, and information technology/information security policies, procedures, and guidelines. In addition, any entity seeking to engage a Vendor should seek legal counsel for advice concerning the specific legal requirements applicable to the entity that impact its vendor analysis and selection approach.