Vendors Checklist

When you're thinking about working with another company (a vendor or third party), it's like inviting someone into your home. You want to make sure they're trustworthy, especially if they'll handle important or private information. You can do as many of these as you feel necessary based on how they are interacting with your data.

1. Get to Know Them

Look Them Up

- **Online Research:** Search online for information about the company. Visit their website, check social media profiles, and read reviews on sites like Glassdoor, Trustpilot, and Yelp. This will give you an idea of their reputation.
- **Example:** Use Google to find news articles, customer reviews, or press releases that mention the vendor.

Ask for Stories

- **Case Studies:** Request examples or case studies of their work, especially where they needed to handle private information securely. This helps you understand their experience and reliability.
- **Example:** Ask for a case study on how they managed a project involving sensitive customer data.

2. Ask the Right Questions

How Do They Keep Data Safe?

- **Data Protection Measures:** Ask about their data protection measures. This includes encryption, access controls, and data backup procedures. It's like asking about their locks and alarms - but for data.
- **Example:** "Can you describe your data encryption methods and how you control access to sensitive information?"

What Happens if Something Goes Wrong?

- **Incident Response Plan:** Find out what their plan is if they encounter a problem, like a data leak. This includes how they detect breaches, their response time, and notification procedures.

- **Example:** "What is your process for handling a data breach, and how quickly do you notify affected parties?" You usually want to make sure that they have a plan in place and that they are obligated under your contract to let you know if any data is compromised.

3. Check their Homework

Proof of Good Behavior

- **Certifications:** Ask if they have any certifications or badges from reputable organizations that show they're good at protecting data. Common certifications include ISO27001 (information security management) and SOC II (security, availability, processing integrity, confidentiality, and privacy).
- **Example:** "Do you have any industry certifications, such as ISO27001 or SOC II, that demonstrate your commitment to data security?"

References

- **Client References:** Ask for contacts from other businesses they've worked with. Reach out and ask about their experience. It's like getting a recommendation for a good movie.
- **Example:** "Can you provide references from current or past clients who can speak to your data protection practices?"

4. Look at the Legal Stuff

Read the Fine Print

- **Policies and Terms:** If they have policies or terms of service, read them thoroughly. Look specifically at how they handle data privacy and security.
- **Example:** "Could you provide your terms of service and privacy policy? We need to understand how you handle and protect data."

Agreements

- **Contract Clauses:** Ensure any contracts include clear clauses about data protection, confidentiality, and breach response. Make sure the contract specifies what happens if there's a problem.
- **Example:** "We need the contract to include a clause on data protection that outlines how you will safeguard our information and the steps you will take in case of a data breach."

Legal Standing

- **Ongoing Legal Challenges:** Verify that the vendor is properly registered and has no significant legal issues.
- **Example:** "Are there any ongoing legal proceedings or past issues we should be aware of?"

5. Plan for Changes

Stay in Touch

- **Regular Check-Ins:** Set up regular check-ins to discuss how things are going and any new or changing risks. This helps keep the relationship transparent and proactive.

- **Example:** "Let's schedule monthly meetings to review the progress and discuss any potential risks or changes in the project."

Know How to Say Goodbye

- **Termination Plan:** Have a plan for ending the relationship safely, ensuring all your information is returned or properly deleted. Define the steps and responsibilities for both parties.
- **Example:** "In the event of termination, we need a detailed plan for how you will return or securely delete our data. Please include this in the contract."

Making the Decision

- **Trust Your Instincts:** If something feels off, it might be worth reconsidering or asking more questions. Your intuition can be a valuable tool in the decision-making process.
- **Example:** "I noticed a few inconsistencies in their answers. I think we should ask for more details on their incident response process."

Take Your Time

- **Avoid Rushing:** Don't rush into a decision. Take the time to review all the information and ensure you're comfortable and confident in their ability to protect your data.
- **Example: "**Let's take a few more days to review their responses and maybe schedule another meeting to clarify some points before making a final decision."

By following these simple steps, you'll be better equipped to choose a vendor that respects your business's and your customers' privacy, just like you do.

Did you find this useful? Why not upgrade to the Privacy Pro Toolkit

Why Upgrade?

- **Comprehensive Guidance:** The Privacy Pro Toolkit provides detailed steps, templates, and tools to help you implement a robust data privacy framework.
- **Regulatory Compliance:** Ensure your data practices meet the latest legal and regulatory requirements.
- **Enhanced Security:** Learn best practices for protecting sensitive data and minimizing risks.
- **Operational Efficiency:** Improve data management and streamline processes with our expert recommendations.

What's Included in the Privacy Pro Toolkit:

- **Detailed Vendor Management Guide:** Step-by-step instructions for assessing, selecting, and managing vendors to ensure they comply with your data privacy standards.
- **Templates and Tools:** Ready-to-use templates for vendor contracts, data processing agreements, and audit checklists.
- **Best Practices:** Comprehensive best practices for maintaining data security and compliance.
- **Regular Updates:** Access to the latest updates and new guidelines as regulations and best practices evolve.

You can find it here.

Disclaimer
The information provided in this Vendor Checklist is for general informational purposes only. While we strive to keep the information up-to-date and accurate, we make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability, or availability with respect to the checklist or the information, products, services, or related graphics contained in the checklist for any purpose. Any reliance you place on such information is therefore strictly at your own risk. In no event will we be liable for any loss or damage including without limitation, indirect or consequential loss or damage, or any loss or damage whatsoever arising from loss of data or profits arising out of, or in connection with, the use of this checklist. This checklist does not constitute legal advice. For specific advice on how to ensure compliance with data protection laws, please consult a qualified legal professional.