Top Ten Privacy Best Practices for Small Businesses in Indiana

10. ☑ Compliance Requirements:

Determine if you hit the **Indiana Consumer Data Protection Act threshold** (e.g., processing data for 100,000 Indiana residents). If you do, compliance is non-negotiable. If you don't, you still need to secure Hoosier data!

Have customers in other states? Or Countries? Then you might need to comply with those laws too, even if you don't have an office there!

9. Vendor Contracts:

Make sure your cloud providers, CRM, and other vendors are contractually required to protect the personal data you give them. If they mess up, **they pay the fine**, not just you!

8. Data Minimization Policy:

Stop collecting everything! Only collect the data you actually need to do business. If you don't need a customer's favorite Bob Knight memory, **don't ask for it!**

7. Data Deletion Plan:

Establish a schedule to securely destroy old, no-longer-needed data. This complies with Indiana's Data Disposal Law and turns data liability into **data dust!**

6. Employee Training:

Have regular, mandatory training sessions. If your employees can spot a fake ID on a Friday night, they should be able to spot a risky use of personal information (PI) on a Monday morning!

5. Incident Response Plan:

Before it happens, write down the steps you will take immediately when your data gets hacked. **Practice it!** Who calls the Attorney General? Who contacts the customers? No one wants to figure this out while the digital house is on fire!

4. Consent for Sensitive Data:

If you collect "sensitive data" (health, biometrics, precise geolocation), you need **CLEAR AND AFFIRMATIVE CONSENT** first. Treat it like asking to borrow the keys to the company truck: be polite and very clear about what you are going to use it for. Then don't exceed that consent grant—you've made a promise!

3. Consumer Privacy Rights Requests:

You know the saying, “failing to plan is planning to fail”. Don’t be that company the Attorney General picks and puts your CEO in the news. You must have a **Response Plan** mapped out NOW that details how your company will fulfill consumer privacy rights reques ts.

2. 🛒 Know Your Data!:

MAP out all **personal** data your company collects, process, stores, or shares. Note **WHAT** data is collected, **WHERE** is collected and stored, and **WHO** it is shared with. This includes any data collected by cookies, tags, pixels, etc. on your website.

1. 📜 The Easy-to-Read Privacy Notice:

Post a **CLEAR, COMPREHENSIVE, and ACCESSIBLE** Privacy Notice on your website explaining *exactly* what data you collect, why you collect it, and how Indiana consumers can **opt-out** of the sale or use of their data for targeted advertising.