Develop your security checklist

5 ways to ensure your SMB is data compliant

As data privacy legislation becomes the norm, small to medium businesses (SMBs) must ensure they meet their legal obligations to protect this valuable new resource – no matter the scale of their operations.

Data has become a business asset that defines the digital economy, and failure to safeguard your customers' personally identifiable information (PII) can be legally and financially devastating – not to mention the long-term collateral damage it can inflict on your brand.

Effective data security can even be a source of competitive advantage, giving you the edge on your marketplace rivals. With the blurring of international boundaries, your SMB could also be subject to laws that originate in other jurisdictions.

GLOBAL COMPLIANCE AND LEGISLATION

If your SMB operates across international borders, you will need to consider the protection of customer data from a global perspective. It could also mean you re-evaluate your processes, procedures, and the way you handle your customers' information.

In a sign that governments are starting to take data privacy seriously, there has been a flurry of new legislation passed around data-breach notification and protection of customer data. All lay out various compliance requirements and prioritize the protection of consumer data and the responsibility to notify authorities of breaches.

These include the EU's General Data Protection Regulation (GDPR) and Australia's Notifiable Data Breaches (NDB) scheme. And while the US does not have a single national data privacy law, individual states like California have started to legislate with the *California Consumer Privacy Act* (CCPA), which is a "GDPR-like" data privacy bill.

The GDPR has generated significant attention, not least because it applies to businesses and organizations outside the EU. The bottom line is that you need to comply if you offer goods and services in the EU, or if you monitor the behavior of individuals in the EU. Data privacy breaches also carry significant penalties under the GDPR: up to 4 per-cent of a company's annual global turnover, or €20 million, whichever is more.

5 ways to ensure your SMB is data compliant

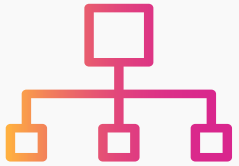
If you run an SMB, it is essential you ensure your operation is compliant. Follow these five tips to make sure you are responsive to both current and future data governance measures, and your data protection practices are current.

1. Treat data as a strategic asset

Treat data as a strategic asset

Start by changing your perception of data: understand that it is an asset that directly affects your business's growth.

This is why you need to develop a data strategy that will enable your business to evolve, thrive, and avoid being constrained by poor data management.



ACTION

Your business is likely to collect more data than you realize, including from sources such as financial institutions and business partners. Start by identifying all the data you hold and own; contact your partners and find out what data they collect and what they can share. Then consider how it can be analyzed for insights to improve your products, services and customer experiences.

2. Compliance is key

Compliance is key

As an SMB owner/operator, you are likely no stranger to compliance, so understanding and adhering to evolving data legislation should be a priority.

You need to manage your data and IT infrastructure to identify any weak points or areas that could be compromised. To be efficient and effective, your data compliance measures should be built into your everyday data-processing activities, and not an ad hoc addition to them.

ACTION

Starting by identifying what is required in your jurisdiction and what will effectively prepare your business for an evolving digital future. Then get familiar with the legislation and its requirements, and develop a risk-assessment checklist to help you stay compliant. You should also develop a risk-aware culture in your workforce. If you don't have the in-house expertise to ensure compliance, get some help. Third-party providers can undertake an assessment to help manage the personal data you hold and advise how best to control and process it.

3. Develop a data strategy

Develop a data strategy

Developing a data strategy helps you clarify when, where, and how all your data is being processed, managed, and stored.

A sound data strategy should include a plan for responding to data breaches to ensure you meet your legal obligations. The more efficiently a breach is dealt with, the less harm to the consumer, the fewer costs incurred and, consequently, the less damage to the reputation of your business. It can also benefit your business if a breach occurs – when determining penalties under the GDPR, for example, a business's compliance and security measures are taken into account.

ACTION

Start by understanding your business's requirements and develop a data strategy that prioritizes the management and security of the personal data you hold. To do this effectively, you need to understand what data you're already gathering and how to process this data for actionable insights. Your strategy should also cover backup, recovery and breach-notification protocols.

4. Make security a priority

Make security a priority

As an SMB owner/operator, the onus is on you to prioritize security in your overall data strategy, and legislation expects a business to have implemented data-protection measures.

Don't fall into the trap of thinking that as an SMB you are not a target for cybercriminals. The PII you hold – including customer data like name, age, date of birth, address, phone number, credit status, employment details, and medical records – is valuable and should be appropriately safeguarded.

ACTION

Take a proactive approach by running an IT audit. Also be aware of what hardware and software requires updating with the latest firmware and security patches. Failure to implement these could leave your business at heightened risk of a security breach. Similarly, analyze your supply chain and cloud providers to ensure they are all compliant.

5. Get the support you need

Get the support you need

SMBs are typically constrained by financial and human resources – so if your jurisdiction's data-privacy requirements are onerous, get some advice and help from experts.

They can help assess and manage the data you hold and advise on future data management, control and processing, and create solutions that meet the relevant legislative requirements.

ACTION

Consult compliance organizations and industry associations for assistance with industry-specific security requirements and solutions. A reputable data security firm can also test and strengthen your IT systems. You may also need to get legal advice if you are not clear what your obligations are, especially if you have a business that operates globally. Prioritizing data privacy is integral to maintaining consumer trust.
By creating a comprehensive data-security strategy, your business can adapt and evolve to an ever-changing legislative environment, and even position itself for growth and new opportunities.

Supplied by VBS iT Services
P: 416-900-6852 | 1-877-709-2656
E: sales@vbsitservices.com
www.vbsitservices.com