ARE YOU DOING ENOUGH TO PROTECT YOUR CUSTOMERS' DATA?

"Companies must embrace their combined responsibilities of using customer data in an ethical way and securing it properly. Proper data hygiene and security need to complement each other, and companies must demonstrate a strong commitment to both to earn and keep consumers' trust. "1

PERSONAL INFORMATION MAY BE VALUABLE TO YOUR BUSINESS, BUT IT'S ALSO SOMETHING CONSUMERS VALUE.

Together we can create a culture of respecting privacy, safeguarding data and enabling trust. Below are key issues to consider when handling personal information.

DO YOU COLLECT PERSONAL INFORMATION THROUGH A WEBSITE?

YES — NO

DO YOU HAVE A PRIVACY STATEMENT?

YES — NO

Ensure that your privacy statement clearly communicates your data use practices and includes contact information and details on who you are and how you collect, use and share personal information.

Communicate clearly and often about what privacy means to your organization and the steps you take to achieve and maintain consumer privacy and security. A privacy policy can be one way to achieve this.

DO YOU COLLECT PERSONAL INFORMATION IN PERSON?

YES — NO

Ensure that the amount and type of data are appropriate to the purpose. Disclose to consumers how you will use the data. Disclose whether you share consumer data. Provide ways for individuals to limit their information use/sharing – and communicate them to consumers.

DO YOU COLLECT PERSONAL INFORMATION FROM THIRD PARTIES AND/OR APPS?

YES — NO

HAVE YOU CONFIRMED THAT EACH SOURCE GOT PERMISSION TO SHARE THE DATA?

YES — NO

In addition to your privacy practices, you are also responsible for how your partners use and collect personal information.

NOW THAT YOU HAVE THOUGHT ABOUT HOW YOU COLLECT INFORMATION, YOU SHOULD CONSIDER HOW THAT INFORMATION IS STORED AND KEPT SECURE.

EVALUATE AND EMPLOY CONTROLS TO PREVENT UNAUTHORIZED ACCESS TO YOUR CONSUMER DATA, WHETHER IT'S KEPT BY A HOSTING SERVICE OR ONSITE.

- Make sure access privileges for all employees and third parties are reviewed and updated regularly.
- Have a written information security policy. Educate employees and third parties on it. Enforce it.
- Require the strongest authentication you can on all sensitive accounts, including multi-factor authentication.

MONITOR AND TRACK THE WAY YOU USE AND MANAGE CONSUMER DATA.

- Monitor the use of personal information so it complies with your privacy disclosures.
- Understand and keep track of user choices before you share personal information with third parties.
- Have a policy that encourages your company to securely dispose of personal information when it is no longer useful

CS4b

CyberSecurity4biz.com

can your business survive without its data?