GTN Newsletter – September 2017

Data Privacy and Security

Craig Dexheimer, Senior Director, Operations / Data Privacy and Security Officer
GTN Shared Services
phone: +1.763.252.0650 | email: cdexheimer@gtn.com

Ransomware, phishing, malware, botnet, viruses, spyware, worms... and the list goes on. You don't have to be an IT specialist to understand that, in our digital world, these data security threats are very real.

As personal data becomes an increasingly vital asset to businesses today, discussions of data privacy and security have graduated from the server room to the boardroom. While the volume (and value) of data processed by companies grows exponentially, so do the risks associated with that data.

As mobile employees travel the world, they expect support from their employer, including safeguarding their personal and confidential information. Companies have a fiduciary responsibility with respect to protecting personal and confidential data of their employees. Part of this responsibility includes working with trusted partners and vendors that are putting data privacy and security at the forefront of their operations.

Is your organization staying ahead of these challenges?

Many companies track the geographic location of their mobile employees. Is the same level of diligence being applied with respect to the security of their personal data, including who has access to that data or where that data is stored?

Have the data security controls implemented by your vendors been reviewed and approved by your organization?

Click here for a simple questionnaire that can be used to evaluate your current vendor's data privacy and security programs: Data Privacy and Security Questionnaire

Consider ensuring partners and vendors that process your mobile employee's Personally Identifiable Information (PII) have taken the following measures:

1. **Established and maintain a privacy policy** that is supported by senior leadership and is reviewed on (at least) a semi-annual basis.

The policy should be made available to the public, easily accessed, and available for review by the individuals whose PII is being processed. The privacy policy should advise individuals what categories of PII is being processed, the purposes for which the data is being processed, the categories of third parties to whom the PII will be made available, and how individuals can contact the organization with any questions or concerns about such processing.

Given the complexity of privacy and cybersecurity law, developing a complete and accurate privacy policy may require assistance from an independent third party advisor.

2. **Obtained an annual System and Organization Controls (SOC) 2 Type 2 audit** from an independent third party auditor.

   This audit examines the controls at a service organization that are relevant to availability, integrity, confidentiality, and privacy. Both the audit and the corresponding report follow the rigorous criteria set forth by the American Institute of Certified Public Accountants. A SOC report allows organizations to provide an independent (and industry standard) assertion that the controls and processes it has implemented are sound.

3. **Engaged a trusted privacy and data security advisor** that can provide expert guidance and structure for an organization's data protection program.

   Regulations around the globe evolve quickly and are becoming more and more stringent. For example, companies conducting business in the European Economic Area will likely be regulated by Europe's sophisticated new privacy law. This new law, the GDPR of the European Union, will become fully effective on May 25, 2018. With the guidance of a reputable third party, an organization will learn how such laws apply to their business and particular circumstances. Such an advisor can also help implement the concept of "privacy by design" which suggests that privacy and security matters should be considered at the outset of any new data-intensive business initiative.

   GTN's privacy and security advisor, Matt Joseph of VeraSafe.com, says, "in the face of a rapidly changing regulatory climate, we encourage our clients to set a high bar – a very high bar – for their own data protection programs. By taking this approach, our clients position themselves well above the high water mark of regulatory fluctuations, thereby avoiding the need to reassess their data protection programs at the onset of each new privacy law. Also, this approach positions our clients as the privacy leaders in their respective industries, which lends a significant commercial advantage."

4. **Appointed a Data Privacy and Security Officer or Data Protection Officer (DPO).** This individual will have the responsibility of overseeing an organization's data protection program, and help ensure compliance with applicable privacy laws.

   It is important to identify a single member within an organization who is ultimately responsible for the protection of the data an organization processes. Doing so will help ensure the chain of command is clearly defined, and the responsibility for data protection isn't confused between various employees. Applicable privacy laws may require the appointment of a DPO who maintains a sense of independence from the organization so that the DPO will be able to independently exercise his or her expertise and judgment, without a conflict of interests. As an

added benefit, the DPO will ideally be able to communicate, both internally and externally, that data privacy and security is a true priority for the organization.

In today's connected world, having a robust data protection program in place is critical. In addition to the tips set forth above, be sure to follow best practices such as to provide all your employees with regular privacy and security training, and have a response plan in place in case you do become the next cybercrime victim.

Are you confident that your global mobility tax services provider is securing and protecting the personal and confidential information of your company and your mobile employees?

CLICK HERE FOR A SIMPLE QUESTIONNAIRE THAT CAN BE USED TO EVALUATE YOUR CURRENT VENDOR'S DATA PRIVACY AND SECURITY PROGRAMS

We encourage you to forward this newsletter to your Data Privacy and Security Officer for further review, and invite you to utilize the questions included in the GTN Data Security Questionnaire to understand your current provider's commitment to data privacy and security.

If you have any further questions regarding the information presented here, or about GTN's data privacy and security program, please contact Craig Dexheimer, Senior Director, Operations / Data Privacy and Security Officer for Global Tax Network at cdexheimer@gtn.com or +1.763.252.0650.

Please see Our Services page for further information on services we offer and tax support we can provide to you and your global mobility program.

The information provided in this newsletter is for general guidance only and should not be utilized in lieu of obtaining professional tax and/or legal advice.