CASE STUDY: RSM HELPS IT SECURITY COMPANY PROACTIVELY ADDRESS GDPR COMPLIANCE

"We are a small legal department, and we simply don't have the resources to take on GDPR on our own. RSM has been a great help—we get along well, and they are hardworking, so we made the transition easily. Most importantly, they had the knowledge of the law and the ability to break down complex concepts into bite-size pieces. It's been phenomenal."

– Jeff Thomas Kowalski, Vice President of Legal, Imprivata

Overview

Imprivata is a leading health care information technology (IT) security company, headquartered in Lexington, Massachusetts. The private equity owned company provides health care organizations around theworld with a platform that addresses critical compliance andsecurity challenges while improving productivity and thepatient experience. Imprivata has more than 1,700 health carecustomers worldwide, serving more than 6 million individualusers across 39 countries.

Background

Imprivata is not based in Europe, but the company has significant operations in the European Union (EU) and is expanding operations on the continent as well as increasing its cloud service offerings. While the company previously sold its software primarily as an on-premises solution, providing the new, additional cloud services requires increased administrative access and entails additional regulatory exposure.

The EU's General Data Protection Regulation (GDPR) requires organizations that handle or process EU personal data to comply with stringent data privacy norms. With Imprivata's move to the cloud, and as a data processor for personal data, its European clients demanded proof of GDPR compliance.

With the GDPR having a direct impact on Imprivata's business, the company needed to understand how much data it had subject to the regulation and how to implement effective GDPR controls.

"Like all companies, Imprivata did not have a choice to comply with GDPR, and we needed to ensure we got the company up to speed on its requirements," said Imprivata's vice president of legal, Jeff Thomas Kowalski. "We have a small legal department, and we simply do not have the resources to tackle GDPR in addition to other privacy and compliance regulations; moreover, we wanted to ensure we had subject matter experts advising us on compliance."

Project

Imprivata chose RSM to help adapt their key processes to GDPR regulations, based on the team's demonstrated success with other GDPR engagements and their global resources to work directly and collaboratively with stakeholders in European countries.

"RSM performed security audits and other compliance work for us in the past and is well-respected in the industry," commented Kowalski. "They were familiar with our business model, and when we coupled that with their great subject matter knowledge, it was an easy decision."

Initially, RSM established a project management office and steering committee to guide the complex work necessary to implement GDPR-compliant processes and controls. Many companies face difficulty managing GDPR and its scope internally, but Imprivata was proactive in taking steps to understand the regulation, become complaint and protect customer data.

RSM then brought together key stakeholders responsible for GDPR compliance for a detailed education session. The seminar covered the complexity of the GDPR from top to bottom, including what it is and what it covers, as well as a projection of how business processes would need to change to achieve compliance.

"RSM's ability to simplify the information needed to ensure we were meeting the GDPR requirements operationally across all internal stakeholders was invaluable to us," said Kowalski.

In addition, the RSM team led a thorough data mapping exercise to help Imprivata organize and assess the data it had access to and how much was subject to GDPR. RSM's global GDPR advisors worked hand in hand with Imprivata to analyze the customer data they possessed, how it is used and how it is processed.

"In my view, data mapping is the most critical piece to the GDPR puzzle," said Kowalski. "RSM was instrumental in simplifying the data mapping process for data stewards (who are not privacy experts) to identify processes and solutions they use that could come in contact with personal data as defined by GDPR. RSM helped establish an online mapping tool and also developed some helpful tips to navigate through the processes that tend to give data stewards issues."

After evaluating Imprivata's customer data and how it was processed, RSM developed a GDPR gap assessment and detailed implementation strategy to determine what was needed to become GDPR compliant. GDPR obligations are extremely broad, ranging from information storage to direct marketing initiatives. RSM worked closely with Imprivata leadership and legal counsel to identify and address any potential compliance gaps and develop a comprehensive GDPR compliance program and infrastructure.

Furthermore, RSM helped Imprivata manage and address some of the misconceptions related to GDPR compliance for operations within Germany regarding data transfers. Leveraging knowledge from RSM Germany, RSM US advisors helped the company understand the GDPR requirements for cross-border data transfers, and established that there was no need for dedicated servers within the country.

"A common misconception with GDPR is that you cannot transfer data outside the European Union," said Kowalski. "The misconception creates a fear that multiple European data centers are needed to conduct business, which, if true, would obviously put strains on our business model. RSM helped clear up the misinterpretation on transfers and helped implement policies to manage those transfers so we can continue to do business in a compliant manner."

Indeed, cross-border data transfers are a critical GDPR compliance area for U.S.-based companies. The GDPR contains stringent requirements for the adequate protection of private data, and the United States is not currently deemed as a country that companies can safely transfer data to, unless the company is a part of the Privacy Shield Framework, or certain contractual provisions are established to safeguard data. RSM worked with Imprivata to help the company become Privacy Shield Framework certified, enabling a safe and compliant transfer of personal data from the EU to the United States.

GDPR compliance is a complex challenge, and many companies do not fully understand how much data they have, or how the law may require changes to existing business processes. Imprivata took a forward-looking approach and brought RSM in to evaluate current policies, develop new compliant procedures, and ultimately create an effective compliance foundation for GDPR and future laws.

"We know new laws are on the horizon, but we all have our eye on the ball," commented Kowalski. "We are discussing next steps with RSM to ensure we have processes in place so we aren't caught off guard when new legislation takes effect. New California laws, as well as other potential U.S. regulations, are a lot like GDPR with some nuances, so I think we are set up to hit the ground running."

Outcomes

RSM's global resources and extensive GDPR experience helped Imprivata implement a comprehensive GDPR compliance program. The RSM team worked collaboratively with company stakeholders and attorneys to understand what data and processes were subject to the law and developed process enhancements to help achieve full compliance. Imprivata's new data privacy foundation enables the company to maintain GDPR-compliant functions to store, process, and transmit customer data both now and in the future, and enables new products and new markets.

Key benefits of RSM's service for Imprivata included:

- Collaborating with management and legal counsel to efficiently achieve GDPR compliance
- Developing an all-inclusive GDPR compliance program
- Creating a data mapping process to successfully navigate processes that contain personal data
- Helping Imprivata become a part of the Privacy Shield Framework for GDPR-compliant data transfer from the EU to the United States
- Implementing a thorough training program, enabling stakeholders to understand their GDPR roles and necessary requirements

+1 800 274 3978
rsmus.com

CS-NT-RAS-ALL-1218