A company undergoing a transition to comply with the GDPR must go through two phases, each with different steps. In phase one a company must find the gap, and then remedy any issues. In phase two, an organization must implement any remedies and then continue to test and monitor them.

First, an organization might realize why they want to be GDPR compliant in the first place. Under the GDPR any enterprise operating within the EU must be compliant with the GDPR even if they do not reside in any of the EU member states. With the global nature of the internet that would mean that it would be in the best interest of any enterprise to comply with these regulations, else they may incur hefty fines for mishandling data.

The first step for a company becoming GDPR compliant is finding the ways in which a company is not complying with the GDPR.This is called the gap analysis. In this phase a consultant may work with the organization to analyze the gaps that may exist in its framework. This means not only the company's internal regulations but also any framework they may have on data protection. A consultant would analyze the current business model including how they transfer, store, and protect data. After identifying the gaps in the organization between its own framework and the legislative requirements of the GDPR, they would move onto the remedial stage.

In this stage a consultant would work with a business to fix the gaps found in the previous step. This would include assessing the cost of the program while building a roadmap or blueprint of the path the company needs to take to achieve compliance and allow a smoother transition.

Entering phase two, the company would begin to transition to a compliant organization. The company would need time to implement the proper training, and build awareness within the company. At every level of the business, the employees must be aware of the legislation that must be followed. Complying with the GDPR is vital anywhere in the company to avoid potentially massive fines. To do this a company must develop internal documentation, and its own ways to enforce the rules with their employees. The company must then monitor the transition to ensure its effectiveness. Finally, the company will enter the last stage of the transition.

In the testing phase, a company will be continually testing to make sure that it's transition into a GDPR compliant company was successful. To do this, they must develop a reliable testing process and perform LiveTesting. A business should also be prepared to adjust the blueprint as needed to ensure that it continues to be effective. Finally, they should have an independent agency give them a report on their companies compliance with the GDPR to ensure that nothing was missed.

Part Two

Under the GDPR, use of data must comply with the following Principles: Lawfulness, Fairness and Transparency, purpose limitation, data minimization, accuracy, storage limitation, and integrity and confidentiality.

The first principle mentioned means that the data must be legally collected and stored under the GDPR regulations, it must be fair and the citizen should know what data has been collected and why it is being collected and used. Under the second Principle, the data must be used only for the purpose of why it was collected in the first

place. The party collecting the data must use the minimal amount of data required. The data also must be reliable, accurate and up to date. The data must also be kept no longer than is strictly necessary. Finally, the data must be handled with proper security protocols and kept private.

The laws governing data in the United States and those in the European Union differ quite a bit. The European Union has much stricter laws when it comes to dealing with data collection laws. For example, in the United States, companies and organizations have no real limit on how long they can hold onto a citizen's data. In the European Union, under the GDPR, they can only hold onto a citizen's data for the minimum amount of time needed. The Laws in the EU favor privacy over profit far more than in the US that has restrictions on personally identifiable information but anything else can be used for purposes like advertising. In the European Union, data cannot be transferred like it is in the United States. The US also lacks strict fines and consequences for breaking the law when it comes to privacy. In the EU, a violation of the GDPR leads to a fine four percent of total profits for the year or twenty million euros, whichever is higher. It's laws like this that will make the owners of companies and organizations truly learn to respect users' data.

There are several positions that need to be clarified before better understanding how the GDPR can be enforced. The first of which is the data controller. The data controller is any party, be it a company, organization, or person who determines the purpose of why data is being collected from the subject. The controller acts largely as a custodian for data, ensuring it is maintained and compliant with the GDPR The data subject is anyone who has identifiable information that can be collected from such data,

examples include identification by username or email, and other ways to tie a person to data whether directly or indirectly. A data protection officer is a required position in an enterprise that will oversee the collection and use of data in a company.

References

Sia Partners. (2020, December 02). Retrieved from https://sia-partners.com/

The principles. (n.d.). Retrieved from http://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/.