Why Are Companies Making The Same Data Privacy Compliance Mistakes? A Blog Post by David Goldenberg

A few thoughts and tips to improve your data compliance regime.

If we look at the recent history of data compliance, there are a variety of major mistakes some of the biggest companies have made when it comes to properly protecting their data. When something goes wrong, not only do the customers (whose data can be exposed) suffer, but the company also has to pay, both directly through fines, and indirectly through lost business.

Despite the fact that the stakes have gotten so high when it comes to data compliance, a recent survey of U.S. companies shows that when it comes to data compliance, many companies haven't learned much from the mistakes of others. Here are some of the common repeating issues, and why companies may still be committing them:

-One of the biggest problems is the fact that many companies are still using manual processes to handle GDPR and CCPA privacy rights requests. The major issue here is that going this route requires potentially dozens of employees to tackle the problem, and having humans manage all these requests creates opportunities for human error.

Between the costs of compliance, training staff, and specialized compliance software, companies surveyed say they spend anywhere from $20,000 to over $1,000,000 in GDPR and CCPA compliance alone.

The alternative here is implementing a more automated privacy management system, which will not only fix the issues faster but solve a lot of the potential risks for human error. However, many companies are concerned about implementing an automated solution because it represents a large investment not just in money, but also in time for onboarding their existing staff. In addition, companies are often worried that the automated system will fail or not be completely compliant.

- Another issue is the broad data collection practices of many companies. Companies often collect a lot of data about customers, much of which is never used by the company. Under the current privacy regimes, compliance costs make collecting this data expensive. In addition, if there is a data breach, exposure of this data will not only create reputational harm, but could result in expensive penalties or lawsuits.

Companies should regularly review the data they collect, and delete any data which is no longer needed for their business.

With all this in mind, you would think that there would be a greater sense of urgency to change workflows and plans.

When it comes to failing to establish proper data compliance protocols, not only are you exposing your company to potential breaches but also risk fines and a huge PR hit in the eyes of your customer base. As a result, any data compliance plans should be complemented with the help of an experienced attorney for maximum protection. In addition, you should be looking at new trends in data compliance to make sure that you are crafting an evergreen plan.