3 Common Misconceptions about GDPR and Data Processing for the Telecom Industry

The GDPR (General Data Privacy Regulation) passed in the European Union (EU) in May of 2018 and is one of the most popular topics of discussion amongst telecom businesses who may or may not conduct business on an international level. Time and time again, businesses and even media publications have stated that GDPR isn't important to them, simply because they're either "not affected" or "not governed" by these regulations. Many hold the perception that GDPR only applies to those in the EU, or those who manage business directly in the EU. There is a misconception that the GDPR does not apply to telecom businesses who do not offer goods or services to EU consumers, or process personal EU data. However, in all these scenarios, the GDPR rules and regulations still apply.

Here are three of the most common misconceptions about GDPR and businesses:

1. My Organization Does Not Process EU Personal Data

One of the first misconceptions about GDPR results from an organization's belief that they do not process personal data from the European Union. However, many people do not understand the full scope of the GDPR definition of personal data. The definition as allocated in the GDPR defines personal data as "anything that can directly or indirectly identify a natural person," which almost all telecom companies store in one way or another. This is in reference to any identifier such as name or identification number, location data or any online identifier such as IP address. Additionally, many fail to realize the definition of processing as defined by the GDPR actually applies to any set of operations performed around data. This includes collecting information on customers, recording, alteration, retrieval of this information, consultation, use, erasure or destruction. Combine the far-reach of modern technology and the number of people living abroad, there's likely information stored somewhere that affects EU citizens.

2. My Organization Does Not Have an EU Presence

GDPR applies to 'controllers' and 'processors'. A controller determines the purposes and means of processing personal data. In other words, the controller is the business that is selling a good or service. If any telecom organization processes any sort of data for a "controller," they are thus considered a "processor" under the GDPR. Any size enterprise that processes data on behalf of their controllers is subject to governance, whether or not the organization in question has a physical presence in the EU. Additionally, any company that is located outside of the EU is still subject to the law if the organization is operating an online business that EU customers can access, interact with or purchase products.

3. My Organization Does Not Offer Goods or Services to EU Customers

Whether or not the telecom agency offers goods or services to the EU does not matter if the organization is again processing for their controllers. This labels the organization as a legal "processor." Data processors include software providers such as Salesforce and Microsoft, call centers, payroll, accounting, and market research firms to name a few. All of these functions within any company are considered departments that store or analyze data in some way. If a EU citizen is affected, they are protected under the GDPR and the company must comply with the legalities surrounding that individual.

So, many companies that do not believe GDPR impacts them, do in fact process data of EU data subjects. What's more, GDPR has created a ground swell of countries and states that have decided to update or

create new regulations that mirror GDPR. So, it is more important than ever for privacy to be a top priority. We recommend establishing a proactive practice of collecting country of residence of the prospects and customers with whom you conduct business. Then, as appropriate, collect consent and communication preferences for each data subject. Today, "unsolicited email" in the EU is an easy target for class action lawsuits, especially as it seems consumer opinion on data protection has become increasingly negative. Organizations today must reconsider whether or not they are governed under the laws of GDPR, as it is likely that they are. The best defense is a good offense, considering ways to collect, store and easily change consent and privacy information should be a top concern for all companies.

About the Author:

Eric V. Holtzclaw is Chief Strategist of PossibleNOW. He's a researcher, writer, serial entrepreneur and challenger-of-conventional wisdom. Check out his book with Wiley Publishing on consumer behavior – Laddering: Unlocking the Potential of Consumer Behavior. Eric helps strategically guide companies with the implementation of enterprise-wide consent and preference management solutions.

About PossibleNOW:

PossibleNOW leverages powerful technology and industry-leading expertise to enable companies to listen to customers, remember what they like and dislike and respond in useful, personalized ways. Its enterprise consent and preference management platform, MyPreferences®, collects customer and prospect preferences, stores them safely and makes them available to any other system or application in the enterprise. PossibleNOW strategic services experts identify opportunities, plan technology deployments, design preference collection interfaces and position clients for a win. MyPreferences is purpose-built to help large, complex organizations gain control over communications, mitigate compliance risk and reduce marketing expenses while improving customer experience and loyalty. For more information, call (800) 585-4888, email info(at)possiblenow(dot)com or visit http://www.possiblenow.com.