# GDPR: General Data Protection Regulation

CRMXchange.com

# GDPR: Imposition of EU Standard Will Have a Ripple Effect on Global Contact Center Operations

For most Americans, the only major ordeal they'll face on Friday, May 25th, 2018 is beating the traffic as they head off for the Memorial Day weekend. But for businesses all over the world, the date looms as the beginning of a new set of complex challenges in how they manage the personal data of millions of citizens of the European Union (EU).

The General Data Protection Regulation (GDPR), which goes into effect on that final Friday of May, is a landmark legislative standard developed to strengthen and unify data protection laws for all individuals within the European Union (EU). It incorporates 99 articles intended to make customers in EU nations feel more secure that companies will protect their personal data in terms of how it is stored and used. In today's global economy, the effects of the regulation will not only impact companies in the US and just about every other nation but will have instant ramifications in the way contact centers interact with EU customers.

Perhaps the most eye-opening implication of GDPR for organizations which experience data breaches and fail to take sufficient measures to prevent them, are the potential consequences. Such businesses could face fines of 20 million euros ($24,560,000) or 4% of annual worldwide revenue for the previous year, whichever sum is higher. According to the GDPR website, "A company can be fined 2% for not having their records in order or not notifying the supervising authority and data subject about a breach or not conducting impact assessment."

Prominent among the rights of EU customers mandated by the new standard, individuals will have the right to make a no-cost demand for:

- Access to all their personal data in a structured digital and commonly used format such as a csv or text file to be provided within one month of request.
- Erasure of all their personal data without excessive delay, also colloquially known as "forget-about-me." This will include all data records and call recordings.

As the front line of communications with customers, contact center agents will field many of these requests and be instrumental in fulfilling them. One key issue that management needs to immediately address is ensuring that their staff is capable of processing and tracking the progress of EU customer requests. Another approach suggested by GDPR to remain in compliance is to provide self-service options, such as providing an online portal for customers to access their information.

What are the implications for US companies and contact centers and how are they preparing to meet the challenges?

Industry groups such as PACE (the Professional Association for Customer Engagement) and proactive solution providers are at the forefront. Robert Kobek, President of CustomerCount, an Indiana-based supplier of customer feedback/surveying applications and Chairman of Government Affairs for PACE, sees concern from association members, many of which are global organizations that do business in the EU. "Companies are aware of the recent data breaches at Saks Fifth Avenue, Sears, and Delta and the worldwide reaction to Facebook releasing customer

# GDPR: Imposition of EU Standard Will Have a Ripple Effect on Global Contact Center Operations

data to Cambridge Analytica for a price.They want to understand how they can keep from being liable to the potential hefty fines that could be levied under the GDPR."

Grafton Potter, VP of Sales, North American for PCI Pal, a specialist in helping contact centers take secure phone payment that adhere to Payment Card Industry Data Security Standards (PCI DSS), also sees a dramatic increase in interest in companies striving to understand GDPR. "If you're a company that does business outside the US, it should be resonating with you. If you do a lot of business in the EU, learning about how it could affect you should already be a top priority."

Kobek sees the imposition of the GDPR as an evolving situation which will present numerous questions of how data is being used, making sanctions difficult to interpret and enforce. "Let's say you're an EU customer calling into a US bank. You ask questions to get an idea if they can help you in the future and the conversation is recorded. So, next time you call, they have some additional information to offer you. Does that count as data? Right now, it could." He sees it as being similar in scope to Do Not Call (DNC) regulations. He believes that there will be gray areas for companies that outsource their contact center operations. "This is a legal issue that has recently been addressed if not entirely settled in the US: it's called vicarious liability. DISH Network was levied with an extremely high fine due to the way some third-party supplier sold their system. The decision is under appeal, but one court has already ruled that they are liable for fraudulent practices."

He also sees parallels to GDPR in the strict Canadian Anti-Spam Laws (CASL) which requires businesses like his to adhere to using specifically proscribed verbiage to obtain continued consent for every survey they send electronically to customers in Canada.

He noted that GDP fines will be based on location within the EU. "If a violation takes place in one EU nation, it will be up to that specific country to determine the fine." He noted that it remains to be seen which nations will be more vigilant in their enforcement. "One of the key criteria that will determine the nature of an infringement is intent: if a company can prove that it has done a compliance audit and that a breach is an isolated incident and technical and organizational steps have been taken to ensure it will not recur, a business may be able to ameliorate the damage or possibly even avoid fines."

"If a business operating an inbound, outbound or omnichannel contact center -- whether it's in-house or outsourced -- is collecting data from EU citizens for the purpose of understanding consumer actions and predicting behavior, they can be held complicit for it being misused under GDPR," said Kobek. "If I were running a contact center, I'd be making an all-out effort to get compliant now." He maintains that there are many good options to accomplish this available in the marketplace, including legal firms offering audits and specific guidance as well as technology solutions.

# GDPR: Imposition of EU Standard Will Have a Ripple Effect on Global Contact Center Operations

One supplier in the vanguard of this effort is contact center industry, Five9, who is now laser-focused on providing services to its customers who do business in the EU to enable GDPR compliance. According to Melinda Bas, Senior Director of Compliance and Technology Risk Management at Five9, they contracted with a 3rd party organization on a multi-step program to evaluate and review the practices, policies and procedures companies need to put in place to be compliant.

"It started with a data visibility project to facilitate customers (data controllers) notifying us of their EU processing activities so we can maintain an accurate report of processing activity as required by the GDPR," said Bas. Five9 also undertook an individual data rights management project to help its customers observe EU consumer forget-about-me requests, a retention management initiative to determine what are the valid business needs to enhance and implement data retention to support such key areas as billing accuracy. In addition, the company is pulling out all the stops to comply with GDPR's requirement to provide state of the art security. This includes incident management to monitor any potential or actual data breach. Five9's technology platform processes the data of EU residents, providing functionalities such as enhanced encryption to keep customer data secure. It also allows critical areas such as password complexity to be configured by the customers. Five9 also addresses contract management to help its customers determine their contract risk exposure and ensure that they are compliant under GDPR structure.

Bas noted that aligning with PCI standards offer a good guideline for having the state-of-the art security required by GDPR. This sentiment was echoed and expanded upon by PCI Pal's Grafton Potter. "PCI DSS should act as a tool to achieve GDPR compliance. If you are compliant with PCI DSS, you are meeting most baseline security control standards of GDPR." PCI DSS and GDPR aim to ensure organizations secure a consumer's personal data but PCI DSS focuses on payment card and cardholder data, while GDPR focuses on all EU personal data including cardholder data. Another key difference is that GDPR provides guidance on what needs protecting but does not provide a detailed action plan. Conversely, PCI DSS is more mature and details clearly what needs to be achieved while providing a clear path with steps and requirements for securing cardholder data."

PCI has penalties in place for repeat offenders. It's a violation if a company experiences a breach and doesn't report it, the organization is breaking the law. Potter believes that following the tenets of PCI provides a path for dealing with people inside EU borders and citizens outside these borders. "If you have a PCI configuration, network infrastructure and a plan, that will make it easier be GDPR compliant," he said.

One key issue that may complicate GDPR enforcement are boundaries surrounding the "forget-about-me" requirements. "In today's environment, people leave data exhaust wherever they go. It may not be a realistic expectation for businesses to have to account for every bit of data," said Kobek.

# GDPR: Imposition of EU Standard Will Have a Ripple Effect on Global Contact Center Operations

Potter concurs, “Does anyone know what is truly personal information? Is it an IP address? Or the cookies you leave when visiting sites? It will be very difficult to account for all of these crumbs of data.”

Finally, there are questions on how violations will be adjudicated for US based companies that are not in compliance with GDPR. If a US company has a branch office in a country where the infraction takes place, that nation’s courts will have jurisdiction. But if a business that operates solely in the US breaks the rules with EU citizens, what legal entity will have the power to enforce the financial penalties? And how will companies with n o legal footing in a specific nation defend themselves effectively? The answers will unfold over time as this evolving standard of GDPR takes effect.