EU GDPR Quick Guide

semafone®
securing data · protecting reputations

What Does The New EU General Data Protection Regulation Mean For You?

The UK has implemented the European Union's General Data Protection Regulation (EU GDPR) which came into effect on 25 May. Post Brexit a new UK Data Protection Bill will come into force, which will help to safeguard citizen's personal data in a new digital age.

Matt Hancock, Secretary of State for Digital, Culture, Media and Sport said:

"The new Data Protection Bill will give us one of the most robust, yet dynamic, set of data laws in the world. The Bill will give people more control over their data, require more consent for its use, and prepare Britain for Brexit. We have some of the best data science in the world and this new law will help it to thrive."

Here's a handy summary of the changes that impact your business:

- **You could face fines of up to 4% of your global turnover or €20m (whichever is the greater)…**
  This is dependent on the severity of the breach and your ability to prove that there were initial measures in place (or not) to protect customer data.
- **…as well as pay-outs to customers**
  On top of the official fines, your company may also be required to pay customers damages in the event of data loss or theft.
- **You need to appoint a Data Protection Officer**
  Whoever holds this position is responsible for managing data protection and data privacy, and free to give recommendations or feedback without fear of negative consequences. *This only applies if you find yourself handling 'significant' volumes of data, and not if you're a small to medium-sized enterprise.*

+44 (0)845 543 0822 emeasales@semafone.com www.semafone.com @semafone Google+ LinkedIn

- **The EU rules apply to anyone trading in Europe**
  Regardless of whether you are headquartered in the EU or not, you still have to comply with the data protection regulations if you offer services within the EU. More generally, the new rules mean tighter controls on protection of data no matter where it is sent, processed or stored.
- **A time limit to report breaches has been set**
  You must report all data breaches to your regulatory body within 72 hours.
- **The laws reach beyond just the one organisation**
  Any organisation or individual that processes data is responsible for its protection. This means that if you provide information to third-parties, they are subject to the EU GDPR.

GDPR for Contact Centres

Call recording is an essential part of most contact centre operations. It makes dispute resolution easier, ensures quality control, discourages fraudulent behaviour for both agent and caller and can be used as an aid in staff training. Under the GDPR, contact centres have to document the lawful basis for their data processing activity and those that use call recording as part of their training / quality control purposes need to ensure they obtain consent from the individual.

Businesses that choose to outsource their contact centre operations to a third party still need to pay attention to GDPR. As the data controller they are required to ensure service providers processing data on their behalf are compliant.

The GDPR goes beyond longstanding regulations such as the Payment Card Industry Data Security Standards (PCI DSS) which exist to protect card data. Under the GDPR, contact centres have to take a much more holistic look at information security and data processing across the board, to ensure customer data and personal identifiable information (PII) is secure and compliant.

So, what's the big picture?

The cost of a data breach can be devastating to a company. Not only can it mean hefty fines, but also a loss of your customers' trust, falling stock prices and in more serious cases, could even mean you have to lay off staff. According to the Ponemon Institute's 2017 research 'The Impact of Data Breaches on Reputation & Share Value' after a data breach is disclosed, stock prices fall an average of 5%. And Semafone's own research showed that 86% of people would be hesitant to do business with a company that had suffered a security breach. With this in mind, can you afford both the reputational risk and monetary cost to your brand and business?

How can Semafone help?

Semafone's philosophy is 'They can't hack what you don't hold.' We provide patented data capture software that prevents personal data from entering your internal contact centre systems. This means that in the event of a data breach, the data is not present and, therefore, cannot be exploited. Not only does this protect you from the risk of fraud and the associated reputational damage, it also ensures you are compliant with industry regulations such as PCI DSS.

Our software uses DTMF masking technology, which allows your customers to type their sensitive details, whether that be payment card numbers, bank details or other numerical personal information, directly into the keypad without having to worry about them being overheard or stolen. This also means they can stay in constant contact with your customer service representative during the entire transaction, which brings a big improvement in your quality of service and customer satisfaction rates.

Contact us now on 0845 543 0822 or emeasales@semafone.com for more information.