GDPR
Getting it
Right

semafone
securing data · protecting reputations

The GDPR Today – 10 Steps to Getting it Right

If you have a contact centre, your business is on the front line when it comes to handling customer data. Personal information floods in through telephone calls, online chat and social media – and all of it needs to be protected in accordance with the GDPR. To make sure that your customer data is safe and your contact centre is on the right side of the regulation, take a look at our ten-step checklist.

1 So What's the Big Picture?

Identify exactly where all your organisation's customer data is held. If you don't already know this, it's time to find out. Map all your systems so that you can keep track of your data's journey from the moment it first enters your organisation. If a customer requests to be removed from your database – using their 'right to be forgotten' – you need to be able to do it completely, and within a month.

2 For Every Customer Record You Hold, Ask Yourself Why?

The more data you hold, the bigger target you are for hackers. Cyber criminals are increasingly using AI and machine learning to create automated systems for phishing and ransomware attacks that learn to defeat security barriers as they spread. To minimise this threat, hold as little personal customer data as possible and make sure you can justify anything you keep. "Just in case" will no longer do.

3 If You Can't Remove It, Encrypt It

Use tokenisation as much as possible. This form of encryption substitutes sensitive data with "tokens", which are data elements that have no meaning. Hold personal information such as email addresses and names separately from all other data, so that complete records only exist when they are actively needed – the rest of the time the token will be of little use to a hacker. However, remember that encryption is no panacea. It adds a layer of protection, but if you can decode it, so can someone else.

4 Data Handling – Less is More

Unburden your staff by applying the principle of "Least Privilege", so they don't find themselves exposed to any data that they don't absolutely need to see. Too often, in a contact centre, agents are given access to a customer's entire record in the CRM database when all they actually need is a name. By limiting this, you can significantly decrease your risk of insider threats.

5 Self–Authentication Sends a Strong Signal to Phone Fraudsters

Implement solutions such as dual-tone multi-frequency (DTMF) masking - which disguises keypad tones – so that customers who are making purchases over the phone can enter their own payment card details into their phone and remain in communication with the call centre agent, who only sees the confirmation of a successful or unsuccessful transaction. This way both parties are protected.

6 Train Your Team

Carry out regular training in basic security procedures such as changing passwords and make sure that employees know what to look out for to identify attackers. Everyone needs to double check email addresses on unfamiliar requests and to investigate any unexpected demands or appeals for personal information. Employees are frequently targeted and can be a business's weakest link when it comes to data protection, so make sure your procedures are robust and up-to-date.

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

7 Outsourcing

Securing and encrypting the customer data you hold is only the first step. If you are working with partners for some aspects of data processing, it's up to you to make sure that their security measures are as robust as yours. This is still essential if they are based overseas, as the transfer of data outside the EU is subject to specific conditions and contracts within GDPR clauses. It is wise to draw up contractual agreements to clarify expectations on all data processing agreements.

8 Keep Records as Though the Customer Will Read Them

Under the GDPR, customers can invoke a Subject Access Request, which can grant them access to the comments logged during a call. This no longer incurs a charge for the customer so the number of requests could rise. Everyone knows how tempting it can be to vent one's feelings in writing on the CRM system after a difficult call, but don't get caught out. Train your team to keep the records professional, or your company's reputation could be in serious trouble.

9 Don't Forget to Protect the Team

Remember that your employees are also protected by the GDPR. If you need to hand over any call information to a customer, remove any details that might identify the call centre agent first. While this could be time-consuming and expensive, re-vamping your systems over time will make this process easier. In the meantime, don't let your eagerness to protect your customers' data overlook the privacy of your team.

10 Privacy by Design

Last, but not least, when developing new systems and products, ensure that teams across your organisation collaborate to apply the principle of "privacy by design" at the earliest opportunity. It is easier and far more cost effective to build in privacy and security at the concept stages rather than bolting this on at the end of the development or production life cycle.

If you'd like to talk to us about how to make your contact centre secure and compliant with EU GDPR and PCI DSS, please email us at emeasales@semafone.com, phone us on 0845 543 0822, or visit www.semafone.com.

semafone®
securing data · protecting reputations

Read our report on compliance with the GDPR, here.