EU GDPR

A GUIDE FOR CONTACT CENTRES
TWELVE STEPS TO COMPLIANCE

semafone®

securing data · protecting reputations

Let's Celebrate the GDPR!

Semafone was set up in 2009 to help contact centres comply with a regulation that was causing the industry a big headache; the Payment Card Industry Data Security Standard (PCI DSS). Almost a decade on, we are seeing the EU General Data Protection Regulation (GDPR) throw up challenges which look familiar. Both regulations are all about protecting customer data and keeping it safe. And both recommend that companies should retain as little sensitive customer data as possible.

This is an approach we endorse whole-heartedly: our own Cardprotect solution is based entirely on the principle that if you don't hold payment card details, they can't be hacked. In our ten years of working with contact centres we have broadened our technology and expertise to handle a wide range of customer data across multiple engagement channels, but the EU GDPR is bringing challenges that many companies are still struggling to understand. We've seen our own clients inundated with offers of new solutions from eager suppliers, many of whom are using stories about fines, lost sales and even prison sentences in order to sell their products and services.

Our point of view is simple. The EU GDPR is a good thing for everyone, and its guidelines represent a better way of working. With such a deluge of information, however, contact centres would benefit from some straightforward guidelines about what it means. We spoke to some industry experts, from both inside Semafone and outside the company, in order to focus on the parts of the EU GDPR that matter most to this sector. We hope this guide will help you to keep your contact centre on the right side of the GDPR, and to keep your customers' data – and your own reputation – safe.

Don't Panic!

The Codification of Common Sense

The contact centre is, by its very nature, all about customer information. It exists so that everyone using your organisation's services – whether they are a shopper, a patient, a local citizen or a member – can exchange information with you. As such, it is one of the key focal points of the European Union General Data Protection Regulation (EU GDPR).

"Regulators want organisations to take better care of customer data – they aren't on a mission to wage war on business or to drive companies overseas"

But the new regulation has been the subject of a great deal of scare-mongering. It's true that the EU GDPR carries the threat of a fine for a data breach that can reach 4% of revenues or €20 million, whichever is greater. It's also true that the "right to be forgotten" is real and that some organisations are now required to appoint a data protection officer. But as Simon Martindill, Head of Marketing at voice, data and infrastructure specialist 360 Solutions, points out, this isn't the whole story. "There's a great deal of misinformation, paranoia and confusion when it comes to the EU GDPR. And a lot of people are just trying to sell services on the back of this uncertainty."

Patrick Cooper, an independent consultant specialising in data and GDPR, and Semafone's own Global Solutions Director, Ben Rafferty, both see the regulation and the Information Commissioner's Office (ICO), which will be overseeing its enforcement in the UK, in a positive light. "The GDPR is a fantastic thing and is overdue," comments Patrick. "Of course people should have control over their own data; it's the codification of common sense." Ben agrees – "The GDPR only contains rules that you should be following in the first place. And regulators want organisations to take better care of customer data – they aren't on a mission to wage war on business or to drive companies overseas."

What About the Fines?

The regulator will have to show its teeth at least a little in order to ensure that the GDPR is taken seriously. Overall, however, as Ben Rafferty explains, the route to compliance is about demonstrating that you are trying to do the right thing. "In the UK, the ICO wants to see that companies are following the spirit of the law as well as the letter." While it can issue fines, it may instead – or as well – serve an enforcement notice to ensure that an organisation takes action and changes a practice that it deems to be putting customer data at risk.

And there is a bright side. For IT departments that have been struggling to gain approval for spending on improvements to security, the GDPR provides a ready-made cost justification.

Where Are We Now?

Storage has been too cheap for too long. For decades it has been far easier to leave customer data where it is than to spend the time and money required to go through every record and clean it up.

Mergers and acquisitions have made things worse as customer records have been accumulated in separate databases. What was once a rich trove of useful information may have morphed over years of neglect into a toxic morass of personal data.

Where to Begin

At its core, the GDPR simply requires organisations to take better care of an individual's personal data. When making any decisions about the handling of someone's information, you must consider the impact on privacy first and foremost. The following points will help you to preserve this privacy.

1

Know what you've got

Start by understanding where your customer data is. Monica Basso, Research VP, and Deborah Kish, Principal Research Analyst at Gartner, in a February 2018 report entitled ***Get Ready for the Impact of GDPR on Content and Collaboration***, advocate a thorough data discovery exercise, followed up by a classification process. They recommend companies "Pursue discovery of personal data across multiple content repositories by using AI and machine learning techniques, such as content and file analysis, automated metadata extraction and classification of content."

Map out your systems and gain an understanding of how much data you hold, where you hold it, and how long you have had it. Track the path of your data from the second it enters your system and understand where it ends up. At no point should records holding personal data simply disappear into an archive. If a customer wants to be removed from your database, you need to be able to do it completely and immediately.

2

For every customer record you hold, ask yourself why

One of the key points of the EU GDPR is that you must have a legitimate reason to be holding the customer's data. Keeping the details of former customers on record simply so you can send them marketing messages won't do.

All of our experts advised that you should start with the assumption that your organisation will be breached. So, if your data was lost or stolen, can you justify why you were holding it? If you are not an accountant, how can you explain keeping someone's financial records? When it comes to ultra-sensitive information such as health information, you need a cast-iron case. In all instances when you're in doubt about whether you should be holding a record, DON'T.

3

If you can't remove it, encrypt it

Simon Martindill considers encryption to be an incomplete solution – if you can de-encrypt your data, so, potentially, can someone else. Preventing sensitive information from entering your environment is preferable. If this is not viable, you can at least make things a lot harder for the fraudsters. Use tokenisation as much as possible, and separate personal information (email addresses, names etc) from all other data. In this way, complete records are assembled only when a record is actively required for the purposes of a specific transaction or query.

4

If it's statistics you need, anonymise everything

If you want to keep customer data for longer than the active life of the requirement, remove the personal information altogether. Patrick Cooper recommends building this into the lifecycle of all data: "Strip away anything that can actively link it to an individual – names, addresses, email addresses – and replace these with a new unique record number. That way, if your data is ever hacked, nobody can be identified."

5

Data handling – less is more

Shane Lewis, Semafone's Information Security Manager, points out that humans are still the weakest link in the chain. "You've got to trust staff," he explains, "but you can help them a lot by always applying the principle of "Least Privilege", so nobody is exposed to any data that they don't need to see. Too often, in a contact centre, new agents will be given access to a customer's entire record in the CRM database when all they need is a name. By limiting this, you can significantly decrease your risk exposure." Ben Rafferty adds that you can take this a step further by authenticating the user first and only then authorising the agent to access the data.

6

Self–authentication keeps agents out of the picture

Shane Lewis sees self-authentication – whereby only the customer can see or hear the information they enter – as another essential element to this process. If the customer is able to enter their own details, while the service agent sees only the confirmation of a successful or unsuccessful transaction, both are protected further from the threat of fraud. With technologies such as DTMF masking, which can disguise key tones, this approach is possible for telephone transactions as well as online.

7

Procedures – train your teams

Regular training in procedures for everyone in the contact centre is essential. Not only do your customer service agents need to be fully competent in the basic procedures such as changing passwords and being aware of phishing and spear phishing attacks, but the contact centre managers must be reviewing access levels regularly and ensuring that policies are kept up to date. "Inform employees about GDPR risks and appropriate behaviour by defining clear policies on usage of corporate content and collaboration services for personal activities," noted Gartner's Monica Basso and Deborah Kish. "Implement security awareness and computer-based training".

8

Call recordings – take extra care

In many ways, the recording of calls is still the Achilles heel of the contact centre. Finding ways of avoiding the capture of sensitive information in recordings has always been a major challenge. The implementation of the EU GDPR means that contact centres now also need to justify why a call needs to be recorded at all. If consent has not been given explicitly, legitimate reasons for recording include legal or contractual requirements, public interest, or the interest of one of the parties, unless this is overruled by the interest of the other. You must also take into account the fact that a customer's right to be forgotten also applies to call recording – something which can be difficult to put into action. You may want to review the length of time for which you hold the data.

9

Get with the right regs

If you are compliant with the Payment Card Industry Data Security Standard (PCI DSS) then you are already halfway there. You'll have the policies in place for handling customers' credit and debit card details, so extending this to include all personal information will not mean starting from scratch. In our view, all contact centres should do more than achieving compliance with the PCI DSS alone. In order to take complete control of information security governance, we recommend structuring a framework for the entire organisation that is audited to the ISO 27001:2013 standard. It is important, however, to distinguish between security and privacy: protecting data from fraudsters does not automatically mean that you are also respecting the privacy of its owner.

10

Outsourcing

The EU GDPR makes it clear that you are still responsible if one of your partners allows a data breach to take place, so make sure you are fully aware of exactly who else is handling any of your customer data. It doesn't matter whether they are based outside the EU – if they are handling the data of EU citizens, the EU GDPR still applies. When selecting the right partner you must ensure that you have robust mechanisms in place to enforce the protection of that data; particularly if they are based overseas. Check that there is an "adequacy" ruling in place that obliges them to adhere to standards that are equivalent to the GDPR, and/or put in place contractual agreements, or Binding Corporate Rules. To make this process easier, the EU provides model clauses that can be used in contracts.

11

Keep records as though the customer will read them

Under the GDPR, customers can invoke a Subject Access Request (SAR) in order to gain access to the comments logged during a call. It will no longer be possible to issue a charge for this so we expect the number of requests to increase significantly. Everyone knows how tempting it is to vent one's feelings in writing after a difficult call, but make sure your team knows that the customer could well end up reading any unpleasant comments.

12

Don't forget to protect the team

Finally, don't forget that your staff also have a right to privacy. If you are handing information over to a customer, make sure that you remove any details that might identify the service agent first. This could be time-consuming and expensive, so think about re-vamping your systems over time in order to make it easier to remove everyone's personal data. In the meantime, don't let your eagerness to protect your customers' data make you violate the privacy of your team.

The Information Commissioner's Office

The Information Commissioner's Office provides EU GDPR checklists and other useful information. Visit it at www.ICO.org.uk

NOTE: This document, while intended to inform about the current data privacy and security challenges experienced by IT companies in the global marketplace, is in no way intended to provide legal advice or to endorse a specific course of action.

We would like to offer our thanks to the experts who have contributed to this guide:

- **Simon Martindill** – Marketing Director, 360 Solutions

- **Patrick Cooper** – Independent Consultant specialising in data and EU GDPR. Certified Practitioner in EU GDPR and Certified ISO27001 Implementor.

- **Ben Rafferty** – Global Solutions Director, Semafone

- **Shane Lewis** – Information Security Manager, Semafone

About Semafone

We are contact centre data security and compliance experts, working closely with enterprises around the world to remove sensitive data from IT and business networks. Our aim is to protect your customers and your company's reputation and to help you comply with industry regulations such as PCI DSS and EU GDPR.

Our Cardprotect™ solutions protect payment card information no matter which channels your customers use to contact you. Cardprotect allows your customers to pay you securely over the phone by entering their credit card details directly into their telephone keypad. From here, the numbers are transmitted straight to the payment processor, so that no details are processed through the contact centre infrastructure. Customer service agents are unable to see or hear card numbers as they're being entered into the keypad, which means that the agent can continue the conversation with the customer and manage any queries that arise.

Our Company

Semafone was founded in a contact centre in 2009 and we now support customers in over 26 countries on five continents. Our customers include AO, AXA, The British Heart Foundation, Rogers Communications, Santander, Sky, TalkTalk and parts of the Virgin Group. And we practice what we preach: Semafone has achieved the four leading security and payment accreditations. We have both ISO 27001:2013 and PA-DSS certification – and we are a PCI DSS Level 1 Service Provider and as well as a registered Visa Level 1 Merchant Agent.

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

📞 0845 543 0822

✉ info@semafone.com

🌐 www.semafone.com

🐦 @semafone

G+ Google+

in LinkedIn

📍 Pannell House, Park Street, Guildford, Surrey, GU1 4HN