E-BOOK

GDPR

Preparing your call centre for GDPR

Hostcomm's guide to achieving and maintaining compliance.

Hostcomm
Business VoIP Solutions

Contents

GDPR can't be ignored 3

Key questions about GDPR 4

1. Processing data 5

2. Storing data 6

3. Call recording 7

4. Responding to requests 8

5. Removing and disclosing records 9

6. Reporting 10

7. The wider value chain 11

Your GDPR basics checklist 12

About the Author

Chris Key, CEO, Hostcomm

Chris is founder and Managing Director of hosted telephony provider Hostcomm. The business was one of the first of its kind in the UK and today offers an unrivalled VoIP network infrastructure. Chris's 20 years' experience in voice and data networking and pursuit of innovative new technologies ensure Hostcomm's services are stable, cost-effective and continuously evolving.

GDPR can't be ignored

If you run an inbound or outbound call centre, you probably already take privacy very seriously.

Beyond your moral obligation to behave responsibly, the UK's own Data Protection Act (DPA) 1998 sets clear expectations for handling personal data. Meanwhile, bodies like Ofcom establish the boundaries of reasonable call centre practices.

The temptation, then, is to underestimate just how much of a seismic shift the EU General Data Protection Regulation (GDPR) is for the average call centre. In fact, it represents the most sweeping changes to the rules around calling and - significantly - the way that non-compliance will be enforced.

Whatever the size of your call centre and whatever the nature of your campaigns, GDPR is unavoidable. By definition, you handle personal data all the time, from call recordings to lists of contacts. Some of this data is generated in-house, while some may be sourced from third-party suppliers or shared with your service provider - but you are at least partly responsible for it all.

In this guide, you'll learn about the basic pillars of GDPR compliance that affect the average call centre - what the regulations entail, what you need to do to achieve compliance, and the consequences you could face if you don't.

Whatever the size of your call centre,

GDPR is unavoidable.

Key questions about GDPR

Thanks to extensive news coverage, most of us have heard of GDPR already. But it can be hard to get to grips with the very basic details about GDPR and why you need to become compliant.

What is GDPR?

The EU General Data Protection Regulation (GDPR) is a set of regulations designed to protect the personal data and privacy of EU citizens. The regulations set clear standards for securing personal data, using it appropriately, and giving citizens more control over who can use their information.

Why is this change necessary?

GDPR is the first comprehensive rethink of EU data protection law since the 1995 EU Data Protection Directive, which the UK's 1998 Data Protection Act was built around. Since then, we have seen the growth of social media and sophisticated data-driven advertising, the adoption of smartphones, and lucrative industries built around the sale of personal data. In short, privacy law had become seriously outdated.

Who is affected?

GDPR compliance is a requirement of any business or organization that handles, stores, or processes the personal data of EU citizens - regardless of where they are based.

What happens if I don't comply?

Increased powers of enforcement are a key element of GDPR. If you are found to be in breach of the regulations, you could be subject to a fine worth 4% of your annual turnover, or €20 million - whichever is greater.

Essential terms

Personal data: Information that could be used to directly or indirectly identify somebody
Data subject: The person that data refers to
Data controller: Anyone that determines why and how personal data should be processed
Data processor: Anyone that processes data (not just the data controller)
Processing: The collection or use of data, including automated processing
Data Protection Officer: Some larger businesses need to appoint a named individual to be responsible for data protection

Non-compliance could lead to fines of 4% of your turnover or €20 million.

Areas to examine

1. Processing data

Before you call a single number, you need to be confident that you have a legal basis for processing that personal data (ie. calling it).

GDPR outlines six possibilities:

1. Consent: The data subject has given clear consent
2. Contract: The processing is necessary for a contract or in forming a contract
3. Legal Obligation: Processing is essential for complying with the law
4. Vital Interests: Processing protects someone’s life
5. Public Task: Processing is necessary for a task that falls under the public interest
6. Legitimate Interest: Processing is necessary for your legitimate interests or the interests of a third party – to such a degree that it outweighs the need for privacy

In many inbound contact centres, you will need to make calls in order to fulfil your part of a contract. In other instances, you will need to seek the consent of your data subjects - and, under GDPR, this must be positive opt-in, not assumed consent or pre-filled tick boxes on your website.

When it comes to cold calling, things are a little more complicated. You’ll need to prove that you have a ‘legitimate interest’ in using the data - that is, your right to run a business outweighs the right of a data subject not to be disturbed at a reasonable time. Providing that you’re already calling in-line with Ofcom guidance - with a low threshold for dropped and abandoned calls - you should be able to make a case for legitimate interest. This will need to be recorded and may need to be presented to auditors or following a complaint.

> Before you call a single number, you need to be confident that you have a legal basis for processing.

Areas to examine

2. Storing data

While the text of the GDPR is frustratingly non-specific, data controllers and data processors must take appropriate steps to keep personal information confidential. This will involve organisational measures (policies and practices) as well as technical systems to protect data.

If you use a hosted dialler, some of your security will be in the hands of your service provider. With that in mind, it's more important than ever to work with a partner that understands IT security, the nature of the latest threats, and how to protect data in storage and in transit.

Key things to look for include:

- Physically secure datacentres
- Firewalls implemented on networks
- Ongoing monitoring
- Encryption

> It's more important than ever to work with a partner that understands IT security.

Areas to examine

3. Call recording

An often forgotten about piece of personal data, your call recordings need special consideration to achieve GDPR compliance. The typical call recording will contain some measure of personal information - and you have little to no control over how much personal data your subjects part with.

With that in mind, every contact centre should have a clear strategy around call recordings under GDPR.

There are two key areas to assess: whether you have a legal basis to record calls and your processes for handling recordings.

Your legal basis for call recording

Until now, most call centres have simply notified data subjects that their calls may be recorded, and assumed consent if the call is allowed to continue. Under GDPR, this isn't good enough.

Your need to monitor agent performance may form the basis of a legitimate interest. However, you need to conduct a balancing test to weigh your commercial interests against your data subject's right to privacy. Alternatively, you can record and store calls based on positive, proactive consent. You dialler can help with technologies like Interactive Voice Response (IVR) that can require a caller to take positive action (by pushing a key) before the recording begins.

Alternatively, you'll need robust processes for storing call recordings securely, disclosing the personal your agents can seek consent over the phone and this can be recorded in your dialler database.€20 million - whichever is greater.

Processing call recordings

Storing personal information for any length of time counts as data processing. As a result, information you hold to data subjects on request, and removing old recordings if a customer withdraws their consent.

Agent training is an important step, but your underlying technology must support them effectively, making compliance as quick and easy as possible.

It's inadequate to state that calls are recorded for training purposes.

Areas to examine

4. Responding to requests

In addition to giving data controllers and data processors more responsibility, GDPR gives data subjects unparalleled rights to access the personal data you hold - and request that it is removed.

If a data subject requests access, you must provide this free of charge within one month.
If a data subject requests removal, this must take place within a reasonable timeframe.
If a data subject requests that their data is rectified, this must take place within one month.

In addition, data subjects can consent to certain types of processing (for example, email contact), while removing consent for others (for example, calling).

Ease of access to personal data

With strict timelines, responding to requests from data subjects depends on the personal data you hold being easily retrievable. While pulling records from a dialler database is typically fast, this isn't always the case with other forms of data like recorded calls.

For the sake of maximising efficiency and keeping your costs controlled, make sure your dialler allows you to search data quickly and easily, ideally bringing all the types of information related to a given data subject together in one place.

Automating your processes

In addition, the use of automation can be an effective way to keep on top of requests from data subjects. If your dialler is integrated with your Customer Relationship Management (CRM) system, you can use call disposition codes to trigger automated workflows in an instant.

As an example, you could configure a disposition for 'Disclose data', which automatically dispatches a copy of the personal data you hold when the call ends. As data subjects become more familiar with their rights and choose to exercise them more often, this can be a useful way to keep on top of your obligations.

Your dialler can help you maximise efficiency and keep your costs controlled.

Areas to examine

5. Removing and disclosing records

It is impossible to improve the value you get from your data lists if you don’t understand their quality. Call disposition codes can help you make sense of how your data translates into call outcomes.

Typically, contact centres focus on the use of dispositioning to assess the performance of agents and campaigns, and present that performance to the centre using a wallboard. However, disposition codes are just as useful in assessing the performance of data lists. In a simple pop-up box, your agents can select the most appropriate call outcome, including options for people who have moved, are deceased, or are otherwise not qualified prospects.

A dialler enables these codes to be easily analysed, so you can uncover patterns that may indicate problems with the data list you are using. For example, a large number of ‘not here’ outcomes may indicate that the list you have paid for is already out of date.

In addition, disposition codes can be fed into your Customer Relationship Management (CRM) system directly. Using these codes, you can then target records that need to be cleansed from the database – keeping the information you and your agents are working with more accurate and up-to-date. And that means a better return on investment by not wasting time and money on records that won’t lead to conversions.

> Contact centres focus on the use of dispositioning to assess the performance of agents and campaigns. However, it is just as useful in assessing the performance of data lists.

Areas to examine

6. Reporting

GDPR compliance isn't just about developing and implementing new procedures around personal information. Your real goal is being able to report on every aspect of how you use data, demonstrating your compliance in the event of an audit, complaint, or data breach.

Your dialler, inbound contact centre solution, and CRM system should work seamlessly together to give you the insight you need into how personal data is used. Ideally, this will include clear information on when you secured a positive opt-in (if relevant) or the rationale behind your decision to process data under the legal basis of 'legitimate interest'.

We'd recommend implementing automated reports that can be built and distributed on a regular basis to key stakeholders. These can then be stored to give you complete insight in the event of an audit.

> Your real goal is to report on every aspect of how you use personal data.

Areas to examine

7. The wider value chain

Finally, it's important to remember the other businesses and organisations that may be involved in your use of personal data. This could include third-party services, your hosted dialler provider, and the company you buy data from.

Within your call centre, you decide how and when data is processed. As a result, you are the data controller - even if your list has come from an external source. This leaves you with the ultimate responsibility for GDPR compliance and data protection.

Consider the complete route that data takes from data subjects to your call centre. Every organisation involved in this process should be vetted for GDPR compliance, effective security, and a good understanding of their responsibilities. That way, you'll avoid the potential disaster of taking responsibility for non-compliant records you were unaware of.

You are the data controller - and ultimately responsible for GDPR compliance, wherever data has come from.

Your GDPR basics checklist

Making calls

- □ Do you have consent to call, is it necessary for a contract, or have you conducted an assessment of your legitimate interest?
- □ Are you calling in a way that minimises the infringement of data subjects' rights to privacy / not to be disturbed?
- □ If your contacts have opted-in, can you demonstrate when this positive opt-in was secured?
- □ Have you trained your agents on responding to requests from data subjects, or securing a positive opt-in for call recording?

Security

- □ Is your network configured with the right technical security to protect data (firewalls, antivirus, etc)?
- □ Is your dialler infrastructure secure (in the case of a hosted dialler, is your service provider's infrastructure secure?)?
- □ Are your agents trained on good security practices to keep personal information secure?

Third parties

- □ Have you discussed GDPR compliance with your data suppliers?
- □ Does your dialler service provider understand their obligations under GDPR?
- □ If you disclose data to third parties as part of your processing, are those third-parties maintaining GDPR compliance?

Visibility

- □ Do you have access to detailed reports that could be used in the event of an audit or following a complaint?
- □ Can you quickly and easily pull personal information in response to subject access requests or removal requests, including call recordings?

Hostcomm: a partner that understands the challenges of GDPR for call centres

Since 2004, Hostcomm has helped inbound contact centres, outbound contact centres, and other businesses with hosted VoIP telephony services and hosted cloud contact centre services. We understand the way you do business and the challenges you're facing around GDPR and other compliance standards.

Using our experience in VoIP telephony, SIP trunking, and hosted predictive diallers, we'll deliver compliant technology you can depend on. We'll help you find the right technology to deliver tangible business benefits.

We'll also support you with the best possible service, from expert consultancy and training to ongoing technical support and advice on issues like GDPR.

All as part of a simple, cloud-based service available for a monthly subscription fee – with no capital expenses.

Find out more at www.hostcomm.co.uk

Front Cover Photo created by natanaelginting / Freepik.com

Let us know your requirements and we'll tailor a demo to fit your needs

☎ 0808 168 4400 / 0203 372 8420

✉ sales@hostcomm.co.uk

www.hostcomm.co.uk

in linkedin.com/company/hostcomm-ltd

twitter.com/Hostcomm

G+ Google+

The Old Convent • 8 Broad Street • Ottery St Mary • Devon EX11 1BZ

Hostcomm Limited is a company registered in England and Wales with company number: 05113945.
Registered Office: The Old Convent. Ottery St Mary, Devon, EX11 1BZ • VAT registered GB837980773

Hostcomm
Business VoIP Solutions