pragma
unified technology

iPECS Reseller Guide to GDPR

iPECS
Your Communications Solution

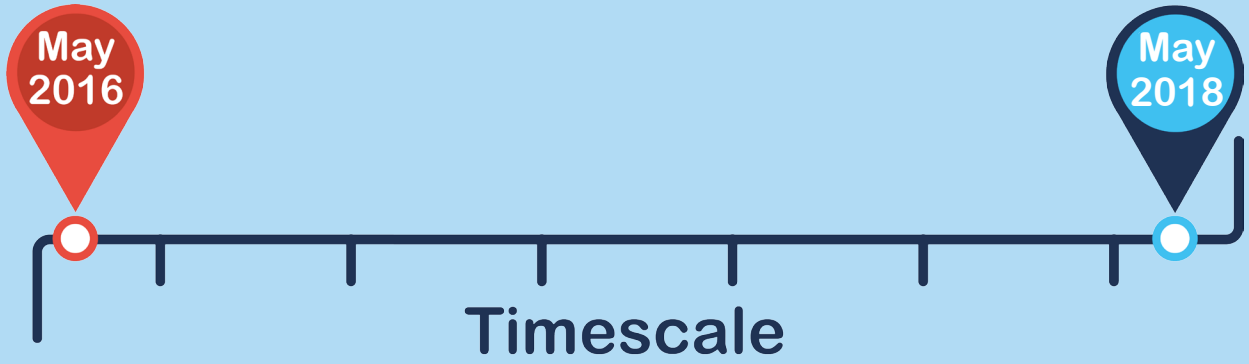
The General Data Protection Regulation (GDPR) has implications for all businesses across the EU that collect personal data. The UK's impending departure from the EU is irrelevant to the rollout of GDPR. Businesses in the UK still need to be GDPR ready and compliant with the new rules to avoid substantial fines. What does all this mean for the telecommunications industry? This article will explore what companies installing or maintaining phone systems should be aware of, and which Ericsson-LG systems may or may not be GDPR ready. Familiar with GDPR? Skip to page 5.

What is GDPR?

General Data Protection Regulation (GDPR) is an amendment to the existing data protection law, defined and enforced by the EU. The purpose of GDPR is to provide protection of personal information for all EU citizens. The new regulations aim to give people more control over their personal data and to make the requirements clear for businesses that handle customer data. It will make businesses more accountable for the way they manage personal data.

Compliance timeline

The two-year transition period began in May 2016, and as of 25th May 2018, GDPR should be fully implemented within every organisation. For an individual member of staff this means they will need to know how to be compliant with their roles and responsibilities when handling a recipient's personal information.[1]



What could happen if I do not comply?

If compliance is breached, fines for small misdemeanours could reach up to £9 million or 2 percent of global annual turnover, whichever is greater. For more serious offences, fines double to £18 million or 4 percent of global annual turnover, whichever is greater.

Source 1 - https://www.metacompliance.com/media/2002/dummiesguide.pdf

The 6 Guiding Principles of GDPR

1. Lawfulness, fairness and transparency

- Lawfulness: Make sure you meet the GDPR lawful basis for processing data.
- Fairness: You must only process data that the recipient has agreed to share.
- Transparency: You must be open and tell the subject how the data is going to be used.

2. Purpose limitation

Personal data can only be obtained for “specified, explicit and legitimate purposes.” [2]

3. Data minimisation

Data should only be stored if it is “adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.” [2]

4. Accuracy

Stored information needs to be “accurate and where necessary kept up-to-date.” [2]

5. Storage limitation

Data should not be held indefinitely and must be “kept in a form which permits identification of data subjects for no longer than necessary.” [2]

6.Confidentiality and integrity

Data should be secure “in a manner ensuring appropriate security of the personal data including protection against unlawful processing or accidental loss, destruction or damage.” [2]

Source 2: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

What does GDPR mean to the telecommunication industry?

How will this affect telecommunication systems?

Almost all phone systems include client data, whether that is an address book holding names and numbers, or a system holding call logs, or call recordings. These are the 3 main areas within most phone systems that could hold information that needs to be GDPR ready. This will include on-premise and cloud-based systems.

Telecommunication providers and resellers should make sure they are installing solutions that are GDPR ready, and any encryption used needs to meet the guidelines.

Contact Information

Most contact information is held within a phone system in plain text format. For a system's contact information to be GDPR ready, the platform should support a level of encryption. The recommended encryption is AES (Advanced Encryption Standard). This is not only the standard for telecommunication manufacturers but is used by most providers within the technology sector to meet GDPR compliance.

Call Logs

Protecting personal information also includes any call logs that are held, even if they are held without any other personal information, such as the person's or business's name. Call logs need to use the same level of AES encryption as outlined in the contact information section in order to be GDPR ready.

Call Recording/Voicemail

All call recordings and voicemails will also need to be encrypted. Businesses wishing to record calls will be required to actively justify legality, by demonstrating the purpose fulfils any of the following six conditions:

1. The people involved in the call have given consent to be recorded
2. Recording is necessary for the fulfilment of a contract
3. Recording is necessary for fulfilling a legal requirement
4. Recording is necessary to protect the interests of one or more participants
5. Recording is in the public interest, or necessary for the exercise of official authority
6. Recording is in the legitimate interests of the recorder, unless those interests are overridden by the interests of the participants in the call

What does GDPR mean for call recording and analytics?

There are many suppliers offering call recording software. Regardless of the supplier, all platforms will need to be GDPR ready.

Tollring provides iCall Suite, a platform for call analytics and call recording, which is fully integrated with Ericsson-LG Unified Communication Platforms. For both resellers and customers, iCall Suite meets all necessary compliance and security obligations.

Businesses using call recording need to focus on which of the 6 processing conditions (outlined on page 5) apply to their business. For general call recording, for example, to monitor service levels or training staff in a contact centre, options 1 and 6 will apply. Therefore businesses must look at how consent is provided and how this consent can be captured for audit purposes.

Gaining consent for call recording

All calls may automatically be recorded, but what happens if the caller does not give you consent? An agent can immediately stop and delete the call recording. Please note, a caller's silence is not classed as consent to record the call.

General rule of thumb for call recording if calls do not fulfil one of the six conditions

Inbound calls

An auto attendant message should inform the customer that their call will be recorded, but only if they wish to be recorded. Customers should inform the agent of their decision regarding consent for call recording when the call is answered. At the point that consent is not granted, the agent can immediately stop and/or delete the call recording thus far.

Outbound calls

When an agent makes an outbound call, they must ask for explicit consent from the caller before the call can be recorded. If explicit consent is not granted you cannot record unless it falls under points 2, 3, 4, or 5.

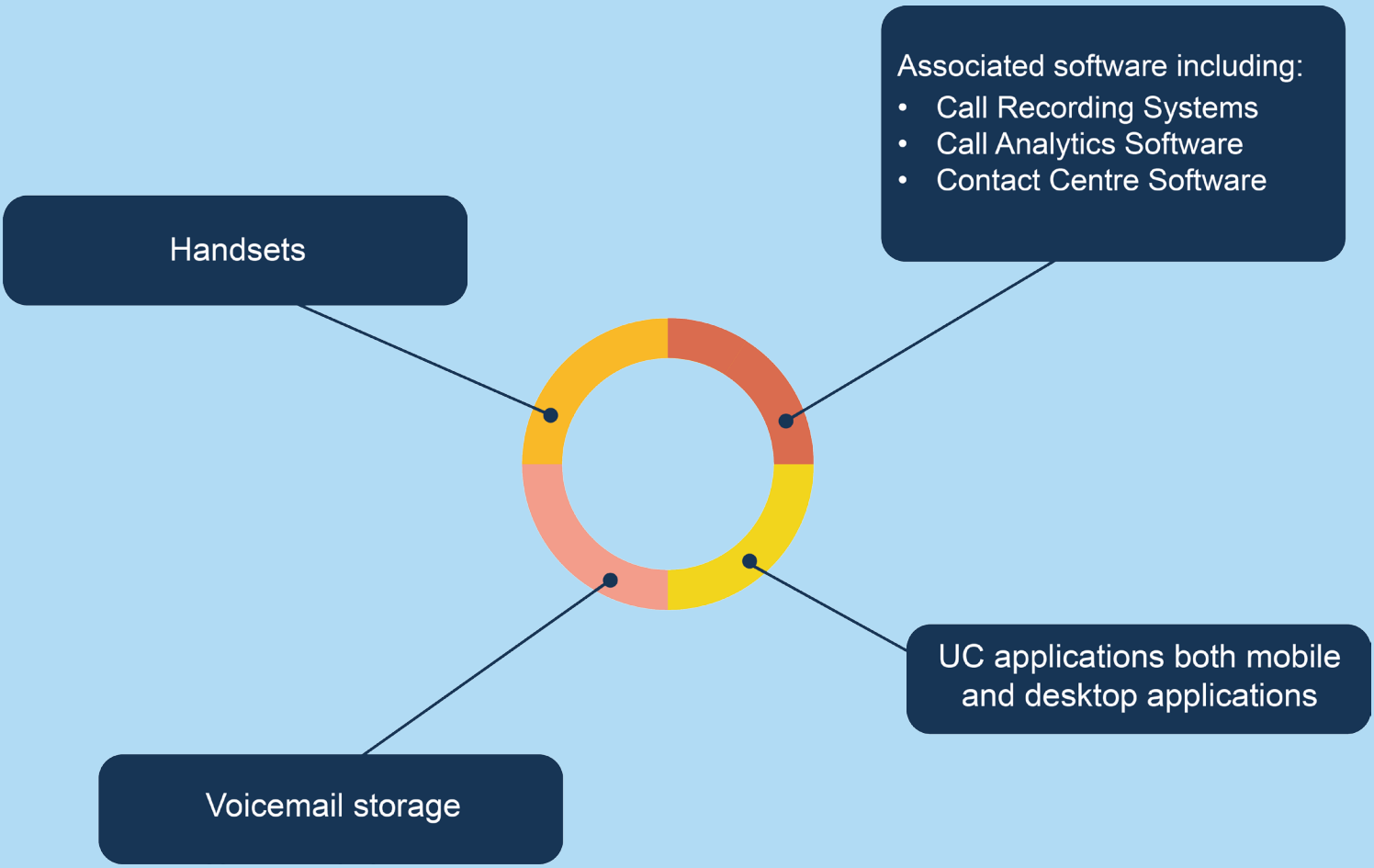
Internal staff

It is advised for businesses to include within their employment contract a clause that states that the use of a business telephone may result in the call being recorded. If staff members wish to make a private or personal call, using a personal phone is recommended.

Software and Hardware that must be GDPR ready

Not only does the core phone system need to be GDPR ready but also any associated hardware, software or applications that hold information need to be compliant with the GDPR guidelines.

This includes:



Here is how an Ericsson-LG system will assist you in being GDPR ready

Since the announcement of GDPR, Ericsson-LG has been working towards being GDPR ready across their current product set. This includes all hardware and software developed by Ericsson-LG and any supported 3rd party software applications. Some legacy systems that are no longer actively developed may require an upgrade to a new system to be GDPR ready.

What systems and hardware will be GDPR ready?

The iPECS product range detailed below will be GDPR ready.
Several systems are already GDPR ready and when this is not the case additional software updates will be released.

Ericsson-LG iPECS hardware and software that will be fully GDPR ready:

Platforms	Applications	Terminals
• iPECS UCM v2.0 • iPECS eMG v3.1 • iPECS UCP v3.1 • iPECS Cloud v3.0	• iPECS UCS v6.1 • iPECS UCE v4.0 • iPECS IP ATTENDANT v3.0 • iPECS IPCR v3.0 • iCall Suite v7.1 • PHONE-LiNK v3.0	• LIP-9000 handset range v2.0 onwards • (DECT) GDC-480H / 500H v3.0 • (IP DECT) GDC-800H v4.2

Ericsson-LG iPECS non-compliant hardware and software:

Platforms
iPECS CM – software upgrade to iPECS UCM required
iPECS LIK - upgrade to iPECS UCP
ipLDK-20 - upgrade to iPECS eMG or UCP

Terminals
iPECS WIT-400HE – upgrade to IP DECT or third party WIFI handset
SIP-8800E – upgrade to LIP-9000 range
LIP 8000E - upgrade to LIP-9000 range
LIP 7000 - upgrade to LIP-9000 range
LDP-9000 - upgrade to LIP-9000 range
LDP-7000 - upgrade to LIP-9000 range
LDP-7200 - upgrade to LIP-9000 range

How Ericsson-LG iPECS is protecting your data

What does GDPR say?

GDPR Recital 83: Controllers and processor should make an evaluation of the risks of their various data processing activities and implement measures to mitigate those risks, such as encryption in order to maintain security and prevent processing that isn't compliant with GDPR.

To meet this requirement AES level encryption will be applied to all areas where personal data is stored. This includes User accounts, contacts, voicemail, call logs, login details/web logins and call recordings.[3]

These will be implemented as part of iPECS Cloud v3.0. No action is required from resellers, all required changes will take place by the manufacturer.

For on-premise systems, an upgrade of the system will need to be performed. Unified v3.1 will have all of the required GDPR enhancements.

Systems and hardware that aren't GDPR ready

Any system that is no longer supported is not GDPR ready and should be upgraded to a new, future-proofed system detailed on page 8.

Other considerations

Request clarification from manufacturers of other software that you may be integrating into your customers phone system, including CRM systems, and other vertical market-based software - accounts software, recruitment software etc. that this software is GDPR compliant.

Being GDPR ready

This paper only covers a generic view of key GDPR issues and those related to telecommunication systems. The most important area to focus on to be GDPR ready are the processes and where necessary complete GDPR training or work with a trained expert in the field.

Useful links:

Information Commissions Office (Source 3)
GDPR For Dummies
EU GDPR

Contact us today for more information on what GDPR means to the telecommunications industry.

www.weare pragma.co.uk

pragma
unified technology