GDPR & VoIP - Burden or Opportunity?

A White Paper from Velona Systems

Tony Friar, Chief Technical Officer

IN DEFENSE OF YOUR BUSINESS VELONA

The opportunity of GDPR & VoIP

GDPR may mostly be seen as a burden for Service Providers, but this paper argues that it represents a significant competitive opportunity (both fixed line and mobile Service Providers) and for Enterprises, particularly call & contact centres, lawyers, and accountants.

Companies who put GDPR solutions in place for their VoIP systems can benefit hugely from GDPR, while improving the defense of their business.

What is GDPR and why it impacts Service Providers and Enterprises?

GDPR is the European Union's new regulatory framework for data protection and privacy and comes into force on the 25th May 2018. GDPR is intended to harmonise data protection laws across the European Union, introducing new obligations on organisations that handle personal data. GDPR defines personal data as anything that can identify a person such as a name, address, phone numbers, IP address, with sensitive personal data, defined as a person's religion, political opinions, genetic information. Voice traffic, specifically VoIP, is by definition, personal data. Insurance offerings increasingly cover VoIP as a subset of Cyber insurance.

GDPR defines Controllers and Processors. The Controller decides the reason for using personal data and how it will be used. The Processor processes the data on behalf of the controller. The Data Controller responsibility passes to the Service Provider with GDPR. Even if the controllers and processors of the data are based outside of the EU the GDPR regulation will still apply to them if they are processing data belonging to EU residents. Companies now face heavy fines if they do not provide adequate protection for personal data.

How can GDPR be an opportunity for Service Providers?

VoIP, for all its flexibility and many advantages over legacy systems, comes with a wide range of vulnerabilities. GDPR now makes it mandatory to address those vulnerabilities, particularly those that can impact on privacy. Presently Service Providers are focused on the IT side of GDPR with less emphasis on the voice side. This brings real opportunities for those Service Providers who are first-to-market with GDPR solutions for VoIP. By implementing GDPR solutions at both the Access and Core Network layers, Service Providers not only better meet GDPR compliance requirements but can also reassure their customers that their privacy is protected. This can be a significant competitive advantage, which over time will become a basic requirement as the impact of GDPR on voice becomes widely known and enforced.

GDPR is not simply a bureaucratic mechanism with no real justification. It provides real privacy protections within a constantly changing digital world and Service Providers who provide real solutions will benefit from improved customer retention, and by attracting new customers, who need the assurance that privacy and data protection are taken seriously by their chosen Service Provider. Enterprise customers such as lawyers,

accountants and call centres who particularly require privacy and confidentiality for their businesses will move to the Service Providers who deliver real GDPR solutions.

GDPR Areas for Concern for Service Providers

The following table highlights the main GDPR areas of concern for Service Providers. Both the Core Network and Access Network have areas of concern within GDPR. It should be noted that even without GDPR the issues below should still be regarded as areas for concern, but GDPR now imposes a regulatory compliance requirement.

Area for concern	Type of Service Provider affected
Voicemail	• All service providers, fixed and mobile, offering Voicemail
Conferencing	• All service providers, fixed and mobile, offering Conferencing
Call Recording	• All service providers, fixed and mobile, offering Call Recording
Interception of calls	• Hosted voice providers including • FMC solutions • SIP trunking providers • Mobile operators • MVNOs
Last number(s) called using VoIP phones	• Hosted voice providers • Fixed Mobile Convergence (FMC) solutions
Fixed Line Access Signalling	• Hosted voice providers including • FMC solutions • SIP trunking providers
Fixed Line Media	• Hosted voice providers including • FMC solutions • SIP trunking providers
VoIP Phone (including softphone) location	• Hosted voice providers • Fixed Mobile Convergence (FMC) solutions
Mobile Location	• Mobile operators • MVNOs
Interception of SMS	• Mobile operators • MVNOs
Malware infected smart phones (various concerns around privacy including call interception, location, access to banking details, etc.)	• Mobile operators • MVNOs • FMC solutions
Monitoring of signalling between 5G network slices	• 5G network providers

The solutions to the above concerns are multi-faceted and require different approaches and solutions to ensure GDPR compliance.

How can GDPR be an opportunity for Enterprise?

The same basic opportunity of GDPR that applies to Service Providers also applies to Enterprise in that those who make and receive phone calls to and from their own customers can now provide extra reassurance to these customers that their privacy is taken seriously and that mechanisms are in place to protect them.

Enterprises such as lawyers, accountants and call centres that depend entirely on privacy and confidentiality for their phone calls need to have GDPR solutions in place. This can be a significant competitive advantage, which over time, will become a basic requirement as the impact of GDPR on voice becomes widely known, and enforced. Presently, Enterprises who are impacted by GDPR are, like the Service Providers, mainly focused on the IT side of GDPR, with the areas of concern on the voice side not being fully addressed. This leaves real opportunities for those Enterprises that can reassure their customers about privacy.

GDPR Areas of Concern for Enterprise

The following table highlights the GDPR areas of concern for Enterprise. It should be noted that even without GDPR these issues should still be regarded as areas for concern, but GDPR now imposes a regulatory compliance requirement.

Area for concern	Type of system affected
Voicemail	• On premise voicemail system, Hosted Voice solution that provides hosted voicemail, mobiles
Conferencing	• On premise conferencing (often part of a PBX or conferencing system), hosted conferencing system
Call Recording	• On premise call recording system, hosted call recording system (sometimes provided as an option with hosted voice systems)
Interception of calls	• PBX, Hosted Voice, SIP Trunking
Last number(s) called using VoIP phones	• PBX, Hosted Voice
Fixed Line Access Signalling	• PBX, Hosted Voice, SIP Trunking
Fixed Line Media	• PBX, Hosted Voice, SIP Trunking
VoIP Phone (including softphone) location	• PBX, Hosted Voice
Mobile Location	• Mobiles
Interception of SMS	• Mobiles
Malware infected smart phones (various concerns around privacy including call interception, location, access to banking details, etc.)	• Mobiles • FMC solutions

The solutions to the above concerns will vary depending on the type of VoIP solution used by the Enterprise. For example, if the Enterprise has an in-house PBX, then responsibility sits with the Enterprise and their PBX maintainer, whereas if they have a Hosted Voice solution then almost all the responsibility sits with the Service Provider. In the case of Hosted Voice solutions, SIP Trunking and mobiles, Enterprises should speak to their Service Provider(s) and ask what specifically is being done about GDPR compliance, and more generally to ensure the privacy of their phone calls, including all the data and media related to this core part of their business.

The current protections are simply not enough

VoIP privacy and security are often not given the priority that is needed. Existing protections are often not sufficient. Standard firewalls and even next generation firewalls do not include the detailed logic and functionality that is needed to protect against even the existing VoIP threats and especially not the future VoIP threats.

Session Border Controllers (SBCs) used in core networks and Enterprise-Session Border Controllers (E-SBCs) used by end businesses are designed to specifically protect VoIP solutions from attacks. SBCs and E-SBCs can be seen as VoIP aware firewalls, but they also frequently fail to protect against even known VoIP threats. The net result is that presently existing mechanisms designed to protect the core network and end businesses can only provide limited protection against VoIP threats and GDPR privacy concerns.

Encryption on the access side between the End Business and the Service Provider or between VoIP phones (including softphones) used by home workers and traveling workers that connect back to the End Businesses PBX is often seen as being all that is needed to provide a secure and private VoIP solution. However, such a belief gives a false sense of security with regards to a number of threats including GDPR privacy related areas. Visibility of the access signalling and media may not be possible if encryption is used but other areas may still be vulnerable (e.g. voicemail, conferencing, mobile location, VoIP Phone location, call interception, etc.). Finally, encryption offers no defence against threats originating from Insiders, since the bad actors here have the required keys, and so are already ‘inside’.

The move to 4G VoLTE and 5G networks, where every call will be VoIP, raises considerable GDPR privacy concerns. Malware infected smartphones can cause various GDPR related privacy problems including call interception, unauthorised recording of calls, unauthorised access to a mobiles location, access to banking details, etc.

Most monitoring systems in current use (where they are used at all), in both Service Providers and End Businesses, do not look for the privacy issues related to GDPR. As such any privacy breach will usually not be detected and known about and may continue for an indefinite time period.

An integrated end-to-end solution is needed to address the complex existing and future VoIP GDPR privacy issues.

Velona's approach to providing GDPR compliance for VoIP

Velona provides a range of products and services for VoIP security to identify and detect GDPR compliance issues.

Threat Management for VoIP

1. Consultancy on GDPR for VoIP.

2. Testing of VoIP solutions (both End Businesses and Service Providers) to check GDPR compliancy.

3. SIP Fingerprinting library (available as an OEM product for C and Java) allows the manufacturer, model and often software version of SIP packets to be identified, so that legitimate and non-legitimate signalling can be easily separated.

4. SIP Malformed Message Detection library (also available as an OEM product for C and Java) allows the identification of not only SIP signalling that is not compliant with the relevant standards, but also the identification of SIP messages that are unusual and could indicate a DoS attack.

5. WATCHER is an off-the-shelf solution that includes SIP Fingerprinting, SIP Malformed Message Detection, Mass Calling Detection, Message Flooding Detection and Toll Fraud Detection and GDPR functionality.

6. CRACKER is a Cloud SaaS Verification and Testing platform to enable MNOs look for weaknesses in SIP security and affordably run Load Testing, and SIP parser / Torture testing so that they can fully verify they are deploying solutions which have the required Advanced Security robustness built in to their deployments.

www.velonasystems.com
(+353) 21 242 8400 | email info@velonasystems.com
Velona Systems Limited, 2nd Floor, 11 Anglesea Street, Cork, Ireland T12 CYR8