GDPR and Real-Time Communications

Part 1: Data Protection Impact Assessments and Data Maps

August 2017

GDPR applies to all applications and services processing personal data. This includes services providing real-time communication such as voice and video calls and Instant Messaging where these services are used to process and transfer personal data. RTC services are at the core of all businesses. Some such as call centres are dedicated to processing personal data, others such as corporate Unified Communication services will inevitably handle personal data at least some of the time.

This white paper from UM Labs outlines a methodology to analysing a corporate RTC service to ensure that it is *GDPR Ready* by the May 2018 deadline.

It cannot have escaped anyone's notice that the European Union's General Data Protection Regulation (European Parliament and the Council of the European Union, 2016) comes into full effect in May 2018. What is less obvious is that GDPR is broad in scope and covers areas and applications which often do not fall within the scope of a cyber security review. A prime example is real-time communications applications running on both IP networks and legacy telecommunications networks.

GDPR applies to the processing of personal data. Article 4.1 of the regulation provides a broad definition of personal data:

> *Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*

Article 4.2 defines data processing to include dissemination and transmission. Guidelines published by the European Union Agency for Network and Information Security (ENISA) for the implementation of EU directives preceding GDPR make it clear that dissemination and transmission includes Real-Time Communication (RTC) services covering PSTN, VoIP, Instant Messaging and all mobile phone networks (ENISA, 2014).

The scope of GDPR and the definition of dissemination and transmission includes a wide range of real-time communications applications *where those applications are involved in processing personal data.* In practice this means that most business orientated use of fixed-line phones connected to the PSTN (Public Switched Telephone Network), call centres, cell-phones, VoIP networks, video calls and Instant Messaging applications are in scope. More specifically the real-time aspects of these services, the call content and call metadata, are in scope.

Article 35 of GDPR defines a requirement to conduct a Data Protection Impact Assessment (DPIA), particularly when new technologies are deployed. As both GDPR and the application of this level of regulatory control to RTC services are new, then a DPIA is required as one of the tasks to ensure that these services are *GDPR Ready* by May 2018. A key element in the task is a data map defining information flows and privacy risks.

This white paper from UM Labs provides a template for a DPIA for Real-Time Communication applications and includes a sample data map. Article 35 of GDPR states that:

> *A single assessment may address a set of similar processing operations that present similar high risks.*

On this basis, the templates provided in this white paper may be used as a starting point for the analysis of a RTC system.

Data Protection Impact Analysis for RTC

Real-Time Communication services differ from other IT applications, as much of the data processed by RTC applications is ephemeral. When an audio or video call is complete there is no residual data unless a call recording application is in place. This means that for RTC the balance between data at rest and data in transit is biased in favour of data in transit. Data in transit includes network traffic transmitted to set up and terminate calls, audio and video streams transmitted during a call and the contents of instant messages sent between the participants of a communication session. The level of personal information included in this data is application dependent, but virtually all systems will carry personal information for at least some of those communication sessions.

At a minimum, a Data Protection Impact Analysis (DPIA) should include the following:

- List of recipients of personal data.
- A description of the purpose of data processing and mechanism used to achieve that processing.
- A definition of the security risks associated with data processing.
- A description of data protection measures incorporated into the system's design or implemented by other applications or services.

The details of each of these topics are dependent on the scope of the RTC system. This can range from a contained corporate Unified Communications service where access is limited to employees, to a system offering public Internet access and links to the global phone network via SIP trunk services.

Recipients of Personal Data

Depending on the scope of the RTC system, the list of data recipients can be restricted to those uses specifically granted access to the service to an almost unlimited list of users on the public Internet or connected via the global phone network. In the former case the list of users can be generated from the user database controlling access to the RTC system. Effective data protection measures can then limit the flow of personal data to identified and authenticated users. In the second case, data protection measures can at best provide a supporting role, and

other mechanisms such as implementing procedures to positively identify the participants in a two-way or multi-way communication must be implemented.

Data Processing Purpose and Mechanism

The purpose of all RTC services is to provide a real-time communication services such as voice or video calls and conferencing. Other related services, such as Instant Messaging (IM) provide a near real-time service and should be considered as part of a DPIA. There is a board range of business needs driving the provision of RTC services. All of which can potentially involve processing of personal data. RTC services can deliver any of the following function. Many systems will deliver more than one of these functions.

- Provide internal corporate communication
- Provide an inbound or outbound channel for customers and business partners, including call centres
- Provide global Internet communication
- Provide global communication via PSTN

A DPIA should identify the scope of the RTC service.

The data processing mechanism used for RTC services is increasingly based on Internet Protocols whether the service utilises the public Internet or "private" IP circuits (in reality private circuits are rarely truly private). This mechanism exposes RTC systems to a wide range of cyber security risks, any one of which could lead to security breach and loss of data resulting in a GDPR compliance violation.

RTC Security Risks

All RTC systems are exposed to security risks. IP based systems are arguably exposed to a greater range of risks than systems restricted to legacy networks, but systems reliant on legacy PTSN connections are also at risk. In both cases, known security threats risk the loss of both data at rest and data in transit.

The data at rest element in most RTC systems is confined to information such as user identity, authentication credentials and system logs or Call Data Records (CDRs) in telecommunication parlance. These elements all include *information that can identify a natural individual* and therefore fall within the scope of GDPR. In those RTC systems providing an IM service, data at rest can also include pending and delivered messages.

RTC systems differ from other IT services in that much of the data is ephemeral. Unless there is a need for call recording (see below), data generated during a voice of video call exists only for the duration of that call. For these elements security risks apply when data is in transit.

The risks facing IP based systems can be classified in 3 categories:

- IP Network threats, low-level, generic security threats common with other network applications.
- Application Level threats, threats specific to the protocols used to drive RTC applications.
- Content Level threats, threats to the content of RTC services (voice calls, video calls, messages).

While traditional perimeter security countermeasures, such as firewalls, can address the IP network security threats, specialist security controls are needed to address the application and content threats.

There are a large number of security risks facing RTC systems, some of the more significant which can lead directly to the compromise of personal data, are summarised in the following table. There are of course a number of other security risks, such as both low-level and application level DoS attacks which do not directly compromise personal data but which could expose the targeted system to other attacks resulting in a data compromise.

Threat Level	Details	Data at Rest	Data in Transit
Content	Unauthorised call monitoring		✓
Content	Call Hijacking		✓
Content	RTP Injection		✓
Application	Directory harvesting	✓	
Application	Password attacks	✓	✓
Application	Caller ID spoofing	✓	✓
Application	Call Hijacking	✓	✓
Application	Log file compromise	✓	
IP Level	Flooding Attacks	✓	
IP Level	System Penetration	✓	

Security risks for RTC services are not confined to those services running on IP networks. Risks exist on other communication networks including 3G/4G cellular networks and the PSTN. Calls made on 3G/4G networks or made via the PSTN will almost certainly be routed over IP networks once they reach the carrier's network.

Data Protection Measures

The fact that standard perimeter security countermeasures address only a fraction of the threats facing RTC systems means that many RTC systems are poorly protected. Relying on general purpose firewalls or even firewalls which claim to be *SIP Aware* or include a *SIP Application Level Gateway (ALG)* leaves the system unprotected against application level and content level threats thereby risking data loss. Many SIP ALGs also introduce service delivery problems, so much so that the UK's NCCC have published a recommendation that firewall vendors leave their SIP ALGs disabled by default (NICC Standards Limited, 2017).

Effective cyber security for RTC services requires targeted defences protecting against both those threats that directly risk the loss of personal data and threats where data loss is a secondary consequence.

Both GDPR (European Parliament and the Council of the European Union, 2016) and the ENISA technical guidelines (ENISA, 2014) include advice on the data protection measures appropriate to meeting the security requirements. GDPR specifically suggests the use of encryption to protect personal data. The standards based protocols that drive many RTC systems specify an effective encryption mechanism for protecting the data in transit. GDPR imposes significant penalties if personal data is compromised as a result of a security breach. These penalties can be up to €20 Million or 4% of annual turnover which ever is the greater. Higher penalties are imposed if the security breach is found to be the result of failing to implement appropriate data protection measures. For RTC services running on IP networks, the use of encryption for voice calls, video calls and IM should be at the top of the list.

The second white paper in this series shows how UM Labs can ensure that RTC systems are fully protected and ready for GDPR.

Call Recording

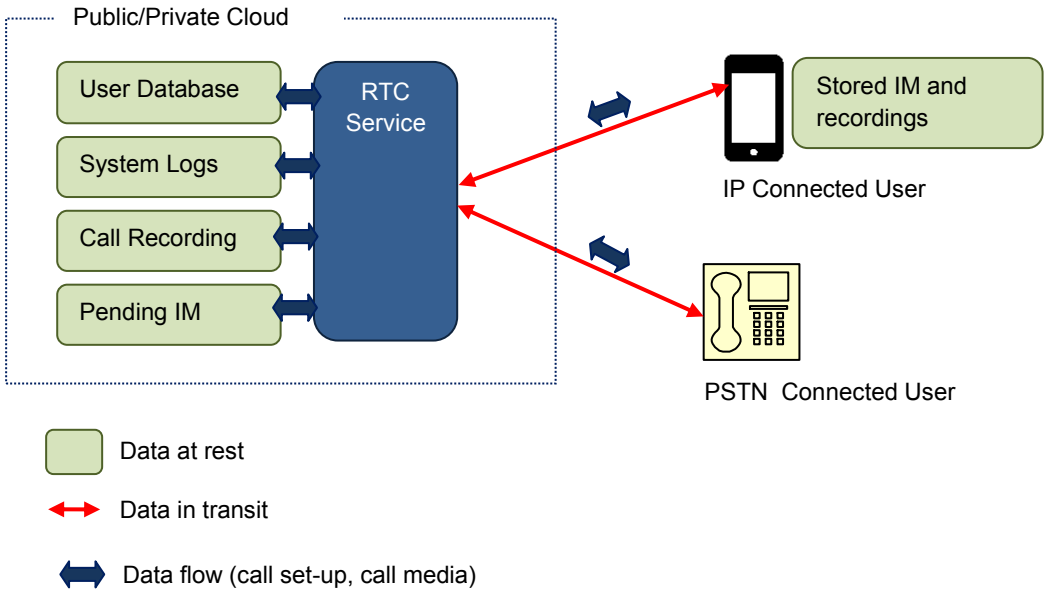
Call recording is not a GDPR requirement, but many organisations processing personal data are also subject to other compliance regulations which require call recording. One of these is MIFID II, which applies directly to investment firms within the European Economic Area (EEA), but includes all trading or execution venues conducting business with the EEA. MIFID II comes into effect on the 3rd of January 2018. GDPR allows call recording where there is a legal requirement to do so, but any call recording system or storage implemented MIFID II compliance must also meet GDPR requirements. This means ensuring that calls are recorded and archived in a way that ensures that personal data in those recordings is fully protected.

Many smartphones and other devices used to connect to RTC applications include a local recording capability. Any call recordings made using this facility fall within the scope of GDPR as they may include personal information. It is obviously more difficult to secure and control local recordings than to control recordings made by a central recording system. One option is to disable the local recording capability through a Mobile Device Management (MDM) application.

RTC Data Maps

Data Mapping is the process of identifying, understanding and mapping out the data flows of an organisation. This exercise provides a framework for the completion of a DPIA as for each identified data flow, the security risks and data protection measures employed to counter those risks can be identified.

A complete data map will detail areas and applications where personal data may be stored, the network paths used for the transmission of data and the data flow within an organisation (for example HR and payroll exchanging personal information on employees). Internal information flows are specific to an individual organisation, but data storage and information flows related to the operation of an RTC service (for example a IP-PBX or UC service) tend to follow a standard model. The following diagram provides a template RTC data map defining the likely information storage points and data flows. This template map provides a starting point for producing a customised data map.



This diagram highlights both data at rest and data in transit. Data at rest elements, which store personal information, include:

- A user database, storing user identity details and authentication credentials.
- System logs which store activity reports including Call Data Records (CDR). CDRs include names or phone numbers which identify and individual and therefore fall within the scope of GDPR
- Call recordings made to meet compliance and legal intercept requirements.
- Pending IM traffic. IM services are not truly real-time, messages may be held on an intermediate system if they cannot be delivered immediately.

Data in transit includes:

- Information transmitted to set up or terminate a communication session
- Information transmitted during a communication session, audio, video and IM.

Some categories of information may appear as both data at rest and data in transit. For example information transmitted to set up a call is normally captured as a CDR, stored CDRs are data at rest. The risks and data protection measures differ for data at rest and data in transit, so information elements occurring in both categories must be represented in each category.

A complete data map must identify all of these elements. The DPIA must then identity the security risks and document the data protection measures applied.

References

ENISA. (2014, December). *Technical Guideline on Security measures for Article 4 and Article 13a*. Retrieved June 5, 2015, from http://tinyurl.com/o5gn28g

European Parliament and the Council of the European Union. (2016, April 27). Retrieved December 6, 2016, from http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

NICC Standards Limited. (2017, March). *ND1440.* Retrieved August 21, 2017, from http://www.niccstandards.org.uk/files/current/ND1440V1.1.1.pdf