TOLLRING

Tollring GDPR Product Update

For Desktop Deployments

February 2018

www.tollring.com

Confidentiality

Version Control

Document Name:	Tollring GDPR Product Update for Desktop Deployments
Description:	Tollring GDPR Product Update for Desktop Deployments
Document Owner(s)	Phil Regan
Document Author:	Phil Regan
Creation Date	26th February 2018
Version number	1.0

Change History

Version	Date	Changed by	Main Changes
Draft	20/02/18	H Oliver	Original Document
1.0	26/02/18	H Oliver	Published Document

Contents

Tollring GDPR Product Update for Desktop Deployments

Introduction

Please refer to the 'Tollring GDPR Update' document published in December 2017 to fully understand the impact of GDPR on Tollring, its partners and customers.

The preservation and protection of private data has been core to our products for over a decade and this has been recognised through our early adoption of the Data Protection Act (DPA) requirements and the acquisition of our ISO9001 and ISO27001 certifications focusing on Quality and Information Security. Please refer to our Data Protection Policy for further details (last updated 10/11/17).

Tollring is taking a stepped approach to ensure that all areas of our products and business are fit for purpose and going forward offer efficient reliable products which maintain the regulatory environment created by GDPR.

This document details planned product changes designed to facilitate compliance, which will be made available in Release 7.1 in May 2018.

Tollring Facilitates Compliance for the Controller

When you or one of your customers subscribe to Tollring's call recording or business analytics services as part of your own business requirements, it is very important that users understand GDPR in the context of their specific business. As a Processor of your data it is our responsibility to ensure that end user data adheres to GDPR requirements ensuring all our compliance and security obligations are fulfilled; it is up to our end customer users to ensure they use the service in a compliant way. Tollring will provide users with the necessary tools within the product to assist them in adhering to the Regulation.

Product Enhancements

Tollring is a provider of call analytics and call recording solutions that are sold via Channel Partners. We need to make sure that we can provide the necessary tools to both our Partners and the end users of our solutions, such that they can meet their compliance obligations. We also need to make sure that where we, as Tollring, store call recordings, as part of the service, that these meet all necessary compliance and security obligations.

Compliance Managers

Release 7.1 will include an executable file specifically for call reporting and/or call recording compliance, supplied as a client license. For security reasons, the 'Compliance Centre' is accessed via the server (or client license) and not via the main desktop application.

An organisation can purchase multiple compliance client licenses, which will be solely for the use of authorised users ('Compliance Managers'). Installation and User Training will be available in order for users to be able to configure their policy rules in accordance to Company requirements.

Call Recording and GDPR

Businesses wishing to record data will be required to actively justify legality, by demonstrating the purpose fulfils any of 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.

This means that businesses who use call recording need to draw up specific policies and procedures outlining which of the processing conditions above they believe applies to them and where necessary explain how they will gain consent from participants.

For general call recording, for example, to monitor service levels or for staff training in a contact centre, the options left to businesses will be numbers one or six. And as the 'legitimate interests' of a business to evaluate customer service are not likely to outweigh the interests of personal privacy under the new regulations, realistically that only leaves gaining consent from all participants as a necessary requirement. Businesses must therefore look at how consent is provided and how this consent can be captured for audit purposes.

Gaining Consent for Call Recording

Our call recording software will record all calls as specified by the business' Policy Rules in Configuration. If consent by the caller is not provided, an agent will be able to stop the call from being recorded immediately by dialling the DTMF call recording pause code.

Education is required to help agents understand their Company call recording business policy. Depending on which of the six conditions the purpose of the call fulfils will determine whether the agent should seek consent from the caller. For general call recording purposes, the following processes should be followed:

Inbound Calls

An auto attendant message should inform the customer that their call will be recorded, but only if they wish to be recorded, and they should inform the agent when the call is answered. At the point that consent is not granted, the agent can immediately stop the call from being recorded using either the DTMF call recording pause code in order to keep a record of the caller's decision, or to reject the entire call recording completely using a DTMF reject code.

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 the caller objects to the call being recorded, the agent can immediately stop the call from being recorded using either the DTMF call recording pause code in order to keep a record of the caller's decision, or to reject the entire call recording completely using a DTMF reject code.

Internal Staff

It is advised that every business should include within their employment contract a clause that states the use of a business telephone may result in the call being recorded and for staff members wishing to make a private or personal call not to use the business telephone.

Compliance Centre Functionality

There are 4 areas to the Compliance Centre:

1. Home Dashboard
2. Policy Rules
3. Delete Call Recordings
4. Audit Reports

Home Dashboard

For **call reporting only**, this section will show the total CLI exclusions and the table of the last 10 audit logs.

For **call recording customers**, the Compliance Dashboard provides an 'at a glance' view of the company compliance policy and statistics.

Filters enable Compliance Managers to view the data on this dashboard based on a specific date range or department.

The **Call Recording Summary** shows statistics based on the following criteria, with links through to relevant data (with filters applied):

- Total Calls Recorded
- Total Calls Excluded
- Total Incoming Calls

- Total Outgoing Calls

Observations provide a summary of the following, with links through to relevant data (with filters applied):

- Total CLI Call Reporting Exclusions
- Total DDI Numbers Not Recorded
- Total CLI Numbers Not Recorded
- Total Whitelisted DDI Numbers
- Total Deleted Call Recordings
- List of Call Recordings

A table shows the **last 10 audit logs** published.

Policy Rules

For **call reporting licenses (no call recording)**, this section will show the CLI call reporting exclusions (add / edit / delete).

For **call recording customers**, this section enables a company compliance policy to be created by applying the following rules to departments within the organisation. **Please note**: If a specific rule is required for a specific extension within the business, that particular extension would need to be in its own department.

Exceptions by department can be applied to the following rules:

- **Record Outgoing Calls**: Yes / No
- **Record Incoming Calls**: Yes / No
- **Exclude CLI from Call Reports**: Add / edit / delete CLI number(s) from the list of exclusions from call data. In this section, telephone numbers can be added to a list of exclusions so in call data within the application the final 6 digits of their number are replaced with 'xxxxxx'. This amended data will remain in the system to avoid inconsistencies in call statistics. This area of the product is only available to users with permission to manage compliance.
- **DDI Call Recording Exclusions**: Add / edit / delete DDI number(s) from the list of exclusions from call recording.
- **CLI Call Recording Exclusions**: Add / edit / delete CLI number(s) from the list of exclusions from call recording. Selection of CLIs based on Customer Directory also available.
- **DDI Call Recording Whitelist**: Add / edit / delete DDI number(s) from the whitelist of DDIs that should always be recorded (for example because of contractual obligations). Adding a DDI to the whitelist will override other exclusions that may have been applied in the policy, such as 'Record Incoming Calls: No' and CLIs listed in the CLI call recording exclusion list.

Delete Call Recordings

This section enables call recordings to be deleted, either individually or in bulk. **This section will not appear on a call reporting only license compliance centre.**

Use a filter to search for the call recording by date range / CLI then select all or select individual call recording(s) to delete.

All associated data will be deleted. Call recording and analytics data will remain in the system with the final 6 digits of any number being replaced with 'xxxxxx' to avoid inconsistencies in call statistics.

When deleting call recordings, the user has the option to add the affected CLI to the exclusion list in Policy Rules.

Proof of deletion can be obtained by running an Audit Report and exporting it as a PDF.

Extension Archiving

Archiving will ensure that a new member of staff using a previous staff member's extension number does not have historic calls assigned to them. For example, extension 235 becomes extension 235_John_001 when archived for audit purposes. Then extension 235 becomes available for the new starter with no call history attached.

Accessed via the Compliance Centre, an extension can be archived. Once archived, the extension will appear in the list of extensions as [extensionnumber_username_sequentialnumber]. All data associated with that extension will be archived. Once archived it will be possible to delete all data then view an audit trail of changes in Audit Reports.

Audit Reports

Filters enable relevant data to be selected then exported as an audit report. It is possible to run reports on usage, deletions and changes across the application.

Timetable for Delivery

Release 7.1 is planned for early May 2018 in time for the GDPR deadline of 25th May 2018. On release, this document will be updated and re-issued with screenshots of functionality enhancements.