PhonEX ONE

GDPR Compliance

Warranty

THE PUBLICATION IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO: THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.

THE PUBLICATION COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN; THESE CHANGES WILL BE INCORPORATED IN NEW EDITIONS OF THE PUBLICATION. MIND CTI LTD. MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S) AND/OR THE PROGRAM(S) DESCRIBED IN THIS PUBLICATION AT ANY TIME.

THIS DOCUMENT IS CONFIDENTIAL AND PROPRIETARY, IS THE EXCLUSIVE PROPERTY OF MIND CTI LTD. AND HAS BEEN PROVIDED FOR REVIEW BY THE RECIPIENT ONLY, AND MAY NOT BE DISCLOSED TO ANY THIRD PARTY. INFORMATION IN THIS DOCUMENT MAY BE SUBJECT TO CHANGE WITHOUT PRIOR NOTICE. NO PART OF THIS DOCUMENT MAY BE REPRODUCED OR TRANSMITTED IN ANY FORM OR BY ANY MEANS WHATSOEVER ELECTRONICALLY OR MECHANICALLY FOR ANY PURPOSE WITHOUT THE EXPRESS WRITTEN PERMISSION OF MIND CTI LTD.

GDPR Compliance

Starting May 25th 2018, GDPR (General Data Protection Regulation) comes into effect. The EU law sets new rules for all companies that get in touch with user data in order to enable digital trust and reduce enterprise risk.

GDPR is aimed to protect EU citizens from data privacy and data breaches in the data-driven continuously evolving applications.

GDPR focuses on the following items: defines the territorial scope (all companies processing the personal data of data subjects residing in the Union), penalties, breach notification (within 72 hours to announce any security risk), right to access (the data controller must give user access for checking for their personal data) and right to be forgotten. The company's activity is coordinated by a DPO (Data Protection Officer) who implements enterprise security model in accordance with GDPR rules.

PhonEX ONE - MIND Trusted Solution

PhonEX ONE UC Analytics and Call Accounting guarantees a high degree of private data security as it collects the right data at the right time with the right purpose. The end-to-end data flow is managed by a ROLE-based, RECORD-based and FIELD-based security.

During the data collection process, the information is safely transferred between sources using secured protocols such as SFTP and RADIUS. Depending on the vendor's capabilities, the collected data can be granularly filtered in such a way that sensitive events will not be transferred (Record-based security).

The PhonEX ONE Collector is part of the CPS (Collect and Process Server) and responsible for configuring the system's sites and data sources. The PhonEX ONE collector, working in the background, is capable of transferring the usage records files by using FTP, SFTP, TCP/IP, Modem, Shared file, ODBC, HTTP, Syslog and Radius protocols and methods.

The key features of the PhonEX ONE collector are:

- Password protected connection
- File transfer recovery mechanism
- Fully safe data transfer
- Backup of transferred data
- Comprehensive logging of the transfer sessions

Data validation and processing is the part where it is decided what personal information is stored into PhonEX ONE MS-SQL proprietary database and how. The security level is strongly implemented in the MS-SQL by user-role access and password protection.

The data validation is made based on the Processor logic and on the driver/plug-in settings. PhonEX ONE processes the call records retrieved from the PBX and stores them in its secured Microsoft SQL database. Each call record received is stored in its raw format in case further investigation is required.

- The system saves data on calls that do not pass user-defined threshold requirements. It is easy to change the threshold parameter and repeat the sorting.
- Undefined lines (the result of different communication problems) are stored in a separate file on a daily basis. This file is used to identify problems and is erased automatically after several days (the amount of days is defined by the user).
- The statistics, the percentage of calls that are below defined thresholds, as well as bad calls are stored on data collection.
- All these tools allow for absolute reliability and avoid data loss.

The organization structure setup and maintenance is established through LDAP SSL which offers a high-degree of protection.

The Maintenance tool is essential for debugging and working with the PhonEX ONE database. This feature is thought to be of great help for the system administrators who maintain the database. Another feature is the automatic maintenance using the system's scheduler. All the actions performed with the Maintenance tools are enabled for the Administrator user rights only. The Maintenance module will allow the administrator to perform several actions such as:

- Archive records;
- Backup records;
- Delete records (enables automatic deletion of CDRs for a user-defined interval)
- Delete jobs (offers the possibility to automatically and periodically delete jobs that have a certain status - *Processed, FailedToProcess or ProcessCancelled* - or are older than a certain number of days/months/years.

User web portal access is ROLE-based (more or less rights are given based on their responsibilities) and FIELD-based (sensitive information including username, address, phone number, dialed number, separation between private and business traffic can be hidden). Moreover, all the operations performed by the user are tracked by the security auditing and logging component of PhonEX ONE.

PhonEX ONE provides a flexible authentication and authorization mechanism that can be **single sign on (SSO), direct validation using Active Directory (AD)** or a **manual process**. For all the cases, the authorization is done using profiles that gives the users more or less rights to access the application resources.

The PhonEX ONE application provides security features that limit all or part of the program to authorized personnel only. The security features can be used to deny access of non-authorized personnel to the PhonEX ONE system parameters, to PhonEX ONE's database, and to specific reporting and query capabilities.

Part of the user's policy is the masking option for dialed numbers, meaning that the dialed number can be entirely or only partially masked (e.g. the last four digits are masked). The masking option is available at user level or for user profiles.

The data retention policy is flexible and adjusted to enterprise's needs.

PhonEX ONE does not place any limitations (by default) in terms of data retention, as long as there is enough disk space at database server level. Still, the user has the option to make backups and archive data (e.g. data older than three years) and restore older events whenever is needed.

The Maintenance tool is essential for debugging and working with the PhonEX ONE database. This feature is thought to be of great help for the system administrators who maintain the database. Another feature is the automatic maintenance using the system's scheduler. All the actions performed with the Maintenance tools are enabled for the Administrator user rights only. The **Maintenance** module will allow the administrator to perform several actions such as: Backup, Delete items, Delete records and Restore.

PhonEX ONE data-driver application is in-line with all the EU GDPR regulations for management and monitoring of personal data.

Raw CDRs are processed and afterwards stored locally on the PhonEX ONE server. The build-in mechanism can be queried for creating CDR backups (on user request or scheduled at regular time intervals). The PhonEX ONE back-end server is built on Microsoft MS-SQL that comes with its own set of back-up tools.

PhonEX ONE system activity can be checked at any moment in time and there are several options to raise alarms in case of malfunctioning: Collection Guardian – no data/ CDRs is received in the last X minutes, Guard – no calls/information processed in the last X minutes, failover/redundancy mechanisms for critical processes (Collector, Processor, Reporting) and comprehensive operations logging.

PhonEX ONE – First-Rate Tool for DPO

The protection of customers' private data against unauthorized or illegal processing, loss or disclosure is very important to us. MIND is ready at all times to provide Data Protection Officers full details about how clients' personal information is collected and used, for which purposes, how longs it is kept and whether personal data can be transferred to other third parties.

PhonEX ONE can utterly disregard the private details or give access to them in a context that is approved by the DPO (except for certain personal details that are required by law, the DPO may freely decide whether or not to give access to any personal data). Customers have the right to access their personal data and can request the rectification, erasure or restriction of use/ processing of their personal data at any time by addressing the DPO in charge.

The Data Protection Officer can benefit of a set of PhonEX ONE features which can help with the implementation of the enterprise security policies. These features allow the Data Protection Officer to:

- Receive alerts on misbehavior (lengthy or costly calls; events outside working hours; forbidden dialed numbers that may pinpoint a communications platform hack/ identity theft)
- Decide on the data retention policy and what should be done with data that does not meet the policy anymore (right to be forgotten)
- Decide what to be collected

- Decide on the private calls classification and the level of protection
- Offer enclosed access to all levels of data (database, web portal)
- Obtain an inventory view (which endpoints and used/ not-used and by whom)