EXTERNAL
Information owner: Information security specialist/Lena Björlin
Reviewed by: CCO/Niclas Haner, CBDO/Magnus Geverts
Approved by: CEO/Olle Düring

TELEOPTI AB

Teleopti Services Information Security Overview

VERSION 1.4

March 7, 2018

Address P.O. Box 24169
SE-104 51 Stockholm, Sweden
Visit Linnégatan 87D

Phone +46 8 568 950 00
E-mail privacy@teleopti.com
Web www.teleopti.com

Contents

1 About the Information Security Overview

- The purpose of this description is to provide an overview of security processes at Teleopti and security features of Teleopti WFM.

2 Teleopti is committed to Information Security

- Information is often the most valuable asset of a company. Our customers also process personal information on their employees, that needs to be handled with care and respect. Therefore, information security is a top priority at Teleopti. The key aspects of Teleopti's information security processes are:
  - Confidentiality – preventing the disclosure of information to unauthorized individuals or systems.
  - Integrity – assuring the accuracy and consistency of data over its entire lifecycle.
  - Availability – ensuring information is available when needed.

3 Information Security regarding Teleopti WFM

- The following provides and overview of security processes and features regarding Teleopti WFM Cloud (hosted services) and Teleopti WFM Product (installed on customer premises).

3.1 Teleopti WFM security features

3.1.1 User access management

- User access is role-based and the access rights of each role is configurable by your system administrator in an easy-to-use administrative interface.
- Teleopti WFM offers the possibility to set up a password policy to increase the access security to user information.
- Federated Single Sign-On using SAML, WS-Federation can be used for authentication in Teleopti WFM Product and dedicated instances of Teleopti WFM Cloud.

3.1.2 Encryption in transit and at rest

- For Teleopti WFM Cloud, all communication channels between user/admin and the Teleopti WFM server and also between database server and the Teleopti WFM server are mandated to use TLS/SSL protocols which enforce both integrity and confidentiality. The same methods could be configured for an on-premise installation.
- Data is encrypted at rest at database level using Transparent Data Encryption (TDE).
- All passwords are hashed and encrypted at row level in the database using a Blowfish/bcrypt encryption algorithm to ensure no clear-text password are sent or stored in the system.

3.1.3 Audit trails and monitoring

- There is an audit trail for changes to schedule data, which can be enabled and disabled by an authorized user. Authorized users can access the audit trail, either as a report or through the *View History* feature in the Schedules module in Teleopti WFM.

- Security audit trails are maintained for connection history in Teleopti WFM and saved in the databases. Only administrators with access to the databases can read them. How long this data should be kept before automatic purge is configurable.
- When hosted in Microsoft Azure, extensive security related auditing and monitoring controls and processes are in place and Teleopti is also monitoring the performance of the service.

3.2 Teleopti WFM Cloud

- Teleopti WFM Cloud is a service hosted in Microsoft Azure. Microsoft provides high levels of availability, network and physical security at their datacenters around the world.
- Microsoft has an extensive security and compliance program for cloud services, including compliance with SOC 1, 2 and 3, Cloud Security Alliance CCM and several certificates such as ISO/IEC 27001 and 22301. The Microsoft Service Trust Portal (microsoft.com/trust) provides independently audited compliance reports as well as information on datacenter security. Independent third-party auditors regularly audit Microsoft datacenters and cloud services.
- Teleopti also utilizes Azure security enhancements like Just In Time (JIT) access to cloud resources and Auditing and Threat detection to further protect the customer installations.

3.2.1 Data Confidentiality and Access management in Azure

- Your Data is always separated from other tenants' data. Tenant-to-tenant isolation is controlled by Azure Active Directory. Isolation is a function of each cloud service's core products and Microsoft product groups regularly test and validate isolation throughout each product's lifecycle.
- Access control is an automated process that follows the principles of separation of duties and granting least privilege, based on user role. For example, system administrators are not provided with database administrative access. This process ensures that the Microsoft administrator requesting access to a customer's IT systems has met specific eligibility requirements. These include a thorough background check to validate previous employment, education, criminal records, etc.; fingerprinting; required security training; and access approvals. The access levels are reviewed periodically to ensure that only individuals with appropriate business justification have access to the systems. Because administrators are personally accountable for their actions, Microsoft also enforce a set of system controls for all access. These include the use of unique user names (for instance, not using "guest" or "administrator"), data access controls, and auditing. Two-factor authentication, such as smart-card logons using digital certificates or RSA tokens, further strengthens the links between specific users and their actions.
- Physical access to Microsoft cloud services datacenters is controlled by two-tier authentication, which includes proxy card access readers (card access badge required) and hand geometry biometric (palm print) readers. Each quarter, an audit is performed to ensure all persons with access still require access and have the least privileged access level necessary to perform their job function. Microsoft has appropriate controls and systems in place to monitor access to the systems and physical hardware within the datacenters, and all such access is tightly controlled and managed. Staff who manage the servers and hardware in Microsoft's datacenters do not have rights to access customer information. Any unwarranted attempts to gain access would be treated as security incidents, and investigated appropriately.
- Microsoft cloud services rely on subcontractors to perform certain support services. Microsoft subcontractors are subject to the same audits as Microsoft itself and are held to the same security and privacy standards as Microsoft employees are, e.g. background checks. Microsoft

will only disclose Your Data to subcontractors if needed to deliver the services Microsoft have retained them to provide. Subcontractors are prohibited from using Your Data for any other purpose, and they are required to maintain the confidentiality of this information. By default, no one has access to Your Data without authorization. Microsoft subcontractors handle your data only when required to provide or maintain the service.

3.2.2 Backup in Azure

- The backup storage geo-replication occurs based on the Azure Storage replication schedule. In Azure storage, the term replication refers to copying files from one location to another. SQL's database replication refers to keeping to multiple secondary databases synchronized with a primary database.
- SQL Database automatically creates database backups and uses Azure read-access geo-redundant storage (RA-GRS) to provide geo-redundancy. These backups are created automatically. Database backups are an essential part of any business continuity and disaster recovery strategy because they protect Your Data from accidental corruption or deletion. Full database backups happen weekly, differential database backups generally happen every few hours, and transaction log backups generally happen every 5 – 10 minutes.

3.2.3 Business Continuity and Disaster Recovery in Microsoft Azure

- Teleopti WFM Cloud leverages the extensive business continuity and disaster recovery program of Microsoft.
- Microsoft has a full enterprise business continuity plan, which includes common scenarios that can endanger the safety or operation of datacenters. Microsoft’s systems are built to automatically failover in the event of large-scale threats or challenges within individual datacenters. The plan incorporates industry best practice across a number of standards.
- From a technology point of view, Microsoft Azure provides an excellent foundation for business continuity. From a data point of view, this includes a built-in high availability subsystem that protects databases from failures of individual servers and devices in a datacenter. Azure SQL Database maintains multiple copies of all data in different physical nodes located across fully independent physical sub-systems to mitigate outages due to failures of individual server components, such as hard drives, network interface adapters, or even entire servers. At any one time, three database replicas are running—one primary replica and two or more secondary replicas. If the hardware fails on the primary replica, Azure SQL Database detects the failure and fails over to the secondary replica. In case of a physical loss of a replica, a new replica is automatically created. So, there are always at minimum two physical, consistent copies of Your Data in the datacenter. Application servers are also automatically replicated to protect customers of failure of an individual server.
- Individual databases and application servers are monitored and automatic alarms are triggered in case of suspected performance issues, to be able to proactively take action and avoid problems for customers. All such alarms are managed 24/7 by Teleopti’s Service Desk. The incident management process defines conditions and routines for escalation to continuity management.

3.3 Teleopti employee access management

- Teleopti staff access is based on their role and work tasks within the company. Access to Your Data is always limited as much as possible both in terms of number of authorized people and their access rights.

- Teleopti's access management procedure requires Our staff to state the purpose of accessing customer environment before gaining access. We use an access management system including password management and traceability features.
- Teleopti's processes for employee onboarding, internal changes, and exit ensures correct access rights. Our access management process also encompasses quarterly review of access roles to correct any inconsistences in access rights.

3.4 Support services

- When supplying support, either remote, or if copying parts of Your Data into our test environment, Teleopti is committed to protecting Your Data. Internal regulations and any additional agreements between You and Teleopti, defines security measures and procedures.
- For technical support Teleopti will use remote connection. Connection information is securely stored in Teleopti's CRM system which is only accessible for approved Teleopti personnel authorized to access Your Data. Passwords are securely stored and managed separately. If physical security tokens are used these are stored in a locked safe.

3.4.1 Access to on-premise installations

- Teleopti WFM Product is installed on Your premises. In this case, Teleopti might perform trouble shooting and support via remote access or at Your location. Remote access will use a VPN connection. Access to customer installations is divided into what is under Teleopti control and what is under Your control. Teleopti access management process governs how access is granted and to whom, and ensures least privileges for our members of staff. You set up personal accounts used for Teleopti access to Your WFM installation, and thus decides on the level of access. In order to connect to Your WFM installation, the authorized member of staff uses a resource for connection information and retrieves the password from a Teleopti password management system. It is possible to set up processes for accounts to be locked by default, requiring a request with a support case reference from Teleopti for it to be opened at Your side. TeamViewer options are also possible.

3.5 Software development

- All software development at Teleopti is performed with high security considerations. Special attention is paid to e.g. validation of input data; authentication and authorization mechanisms, and OWASP top 10.
- An equal essential part of the software development is code reviews to catch any quality or security issues. Teleopti always performs an extra code assessment and/or product review when adding third party components.

3.5.1 Testing

- Teleopti use test-driven development to ensure high quality. The framework is Kanban, an agile method for development. In the Kanban process, each feature goes through our development process of analysis, development and testing. Automated tests run 24/7, whenever code is checked in, and are included in the build chain. When the code has passed all testing, the result is a build, which is automatically deployed in test environments, both on Teleopti premises and in Microsoft Azure. This tests the installation process and ensures that manual testers are always working on the most recent build. In addition to these automated tests, a build will go through several steps before it becomes a release. This includes a mix of automated and manual tests; smoke tests, performance tests, load tests, usability tests and regression tests.

- Teleopti is using two different security scanning services from third-parties to perform daily scans to find any security issues or vulnerabilities. This is integrated into the development build process so that every code change is automatically tested. Testing is done for both on premise installations and cloud installations and the results are sent in a report to our test engineers who reviews it together with Tech lead. Additional manual testing is also carried out.
- External tests, such as penetration tests, are performed at least twice a year and follows OWASP Application Security Verification Standard (ASVS) and evaluates risk of potential vulnerabilities based on Common Weakness Enumeration (CWE).

3.5.2 Update and Upgrade Management

- Teleopti works with continuous delivery to provide corrections, improvements and new functionality to the service. Our processes for maintenance, updates and upgrade management of the WFM services describe aspects such as how to do update/upgrade control, administration of an update/upgrade, test and validation, and how to make roll back if needed.

3.6 Security Incident Management

- Teleopti security incident management process encompasses both customer related and internal security incidents such as data breach and disclosure, non-compliance, illicit data manipulation, malware, and identified vulnerabilities.
- The lifecycle of an incident consists of the first identification, registration and classification, customer notification (and in the event of a personal data breach, authority notification), investigation and diagnosis, resolution and root cause analysis, communication of solution and closure of the incident. The incident management process can be initiated by a customer, a Teleopti employee, or a third-party representative.
- Customer communication is a vital part of the incident management process, in order for customers to receive relevant and timely information, should an incident occur. Incident notification will be made to an Information Security Contact appointed by You.
- Should an incident involve Microsoft Azure, Teleopti will coordinate our actions with representatives from Microsoft to ensure an efficient handling of the incident.
- Teleopti's Information Security Council will review any security incident and the handling thereof to ensure that an appropriate resolution is found and preventive and improving actions are taken. The incident management process defines conditions and routines for escalation to continuity management.

3.7 Data Retention

- Teleopti WFM will automatically purge old data, to comply with regulations and ensure performance of the application. The default retention period for specific types of data is defined in the Service Specification (www.teleopti.com/wfm/legal/service-specification). Adjustments to the standard data retention policy can be agreed upon.

3.8 Expiry and termination of service

- In order to ensure the protection of Your Data, termination of a service agreement is planned and documented so that the risk of unauthorized access to the Your Data is minimized. In accordance with the Service Specification, Your Data will by default be retained for a limited period after the termination of the Master Service Agreement.

- Teleopti has a process to effectively remove all super user rights and administrator rights to the systems which could imply access to Your Data.

4 Privacy and Data Protection

- The processing of personal data is a responsibility, not only for Teleopti as a company but also for every member of our staff. Personal data is always to be processed with respect and consideration. This means not only technical and organizational measures to protect the data, but also that our staff is committed to this responsibility. Privacy and data protection is incorporated into Teleopti's Information Security Management System and part of our training program for all members of staff.
- Protection of personal data and customer related data is of highest priority to Teleopti. Organizational and technical security measures ensure an appropriate level of security, based on information classification and risk assessments.
- When joining Teleopti, each employee signs a confidentiality agreement and is thus committed not to disclose confidential information related to Teleopti, our customers or third parties.

4.1 Compliance with the EU General Data Protection Regulation (GDPR)

- Workforce Management Systems deal with personal information. As a Customer to Us, You are the Personal Data Controller of Your Data and consequently responsible for what data is being put into Teleopti WFM and how it is used. As a Personal Data Controller, You need to make sure that the way your organization uses the WFM-system is compliant with the requirements of the GDPR (EU General Data Protection Regulation).
- Teleopti is committed to provide services that complies with regulations in the EU GDPR, for example concerning privacy by design and default personal data breach notification, and data subjects' rights.
- In order to provide all our customers with great support, Teleopti's support function embrace employees from Sweden, the US and China. Teleopti affiliates are covered by Corporate Clauses.
- Should a personal data breach occur, Teleopti will provide notification and information in order for You (being Personal Data Controller) to notify the supervisory authority in accordance with GDPR requirements. Notification will be made to an Information Security point of contact as appointed by You.

4.1.1 Teleopti WFM Cloud and GDPR

- Teleopti WFM Cloud includes hosting by Teleopti in Microsoft Azure and we ensure that sub-processors have an adequate level of protection and that appropriate safeguards have been put in to place. Teleopti will not engage a sub-processor without prior approval from the personal data controller. Teleopti ensures that any Teleopti affiliate or subcontractor regaining access to or processing personal data has an adequate level of protection and that appropriate safeguards have been put in to place fulfilling the requirements of the GDPR, either under the standard contractual clauses for the transfer of Personal Data to processors established in third countries, as approved by the European Commission in Commission Decision 2010/87/EU of 5th February 2010 ("Standard Contractual Clauses") or having been certified under an approved certification mechanism, such as the EU-US Privacy Shield Framework or any approved certification mechanism replacing Privacy Shield.

- When hosted in Microsoft Azure, the geographical location of Your Data will be restricted to specified Microsoft Azure datacenter(s). Microsoft has datacenters at several locations both within and outside of the EU/EES area.

5 General Security Governance at Teleopti

- Teleopti is currently implementing an Information Security Management System (ISMS) based on the ISO/IEC 27000 standard. An ISMS is a systematic approach to manage the security of assets, including information entrusted to Teleopti by our customers and partners.
- The ISMS covers areas such as: internal regulations for employees (acceptable use policy), information classification, risk management, technical requirements regarding internal IT infrastructure, security incident management, business continuity, disaster recovery, human resource security, security training and awareness, asset management, access control, development and application security, patch management, change management, physical security, third party security management, and compliance/testing/internal audit.
- With support from processes within the ISMS, such as information classification, risk assessment and the so-called plan/do/check/act approach, Teleopti will maintain an appropriate level of security and our personnel will have guidance in their day to day work. The ISMS is designed to support recurring evaluation of the effectiveness of the security measures and based on that make continuous improvements. The ISMS documentation is subject to revision and updates annually or when larger changes affect the scope of each document.
- The following roles are part of the Teleopti information security organization:

Information Security Council	The CEO, Head of IT and the Information Security Specialist forms this council with the purpose of deciding on security related topics and continuously follow up on security related activities.
Information Security Specialist	Responsible for driving and coordinating information security activities and processes. Responsible for implementing, maintaining and continually improving the Teleopti ISMS.
Business Support Specialist with Security focus	Evaluating and improving security related processes within the operations, such as incident management and access management.
IT Security	Part of the IT department responsibilities and daily operations.
Data Protection Coordinator	Responsible for providing support to the organization regarding data protection matters (such as the GDPR), coordinating activities regarding GDPR-compliance, and administrating the data protection management framework.

5.1 Corporate security controls and processes

- As part of the ISMS, Teleopti has an internal security code targeting all employees. The internal security code encompasses areas such as:
  - Introduction and overview of Teleopti's ISMS regarding i.e. objectives, security organization, and ISMS document structure.

- Descriptions of general information security processes such as risk management, information classification, and business continuity management.
- Employees' responsibilities and the acceptable use policy.
- Confidentiality and security aspects of handling customer data.
- Internal requirements, security controls and procedures regarding our IT infrastructure and physical security.
- Security related processes prior to employment, during employment and organizational changes, and at termination of employment.

5.1.1 Background checks of Teleopti employees

- Our recruitment procedure stipulates a minimum of two reference checks to be performed to check reliability, experience and qualifications.
- Screening is made in accordance with national regulations. For US staff, a nationwide criminal search, sex offender search, terrorist watch list, county courthouse criminal search. Social Security numbers are also included. All the criminal data searched covers a 7-year period.

5.1.2 Security awareness and training

- All employees undergo an introduction when joining Teleopti, encompassing internal codes of conduct, the acceptable use policy, and confidentiality concerns. In addition, training related to specific roles, work tasks and current topics (such as GDPR) are performed.

5.1.3 Third party management

- Third parties are assessed regarding aspects such as financial stability, information security program, and personal data protection program.

5.1.4 Business Continuity at Teleopti

- Business Continuity Management at Teleopti is based on the ISO 22301 standard and best practices. Teleopti's overall Business Continuity and Crisis Plan and accompanying Continuity and Disaster Recovery Plans for specific processes and resources are based on a strategic framework and underlying analyses. Teleopti performs regular training of relevant staff and testing of plans. Plans are revised at least annually.

6 Do you want to know more?

- If you have questions on information security or want to know more on a certain information security topic, privacy or GDPR related matter please reach out to us using privacy@teleopti.com.