GateHouse Logistics A/S Security Statement

Document Data

Release date:	11 June 2018
Number of pages:	11
Version:	3.0

Table of Contents

ghTrack ® Security Statement

Purpose

The ghTrack service strives to achieve a high degree of data and communication security as sensitive information may be stored in relation to the usage of ghTrack. To ensure all stakeholders of ghTrack that adequate security measures have been implemented, this document clarifies exactly which measures have been taken in design and production of ghTrack - in relation to data-storage, -backup, -security, -privacy, and international and country-specific regulations, which have to be complied with when handling personal identifiable information or other sensitive telematics related data.

Application

This statement applies to all actors and users of the ghTrack service as a whole. ghTrack is owned, developed, and maintained by the GateHouse Group, under which GateHouse Logistics A/S (VAT No: DK37439541)[1] is an independent legal entity. GateHouse Group is the copyright owner of ghTrack. All users of ghTrack are direct customers of GateHouse Logistics A/S and shall therefore only be bound to user agreements with GateHouse Logistics A/S and its general terms and conditions.

Terms

Customer	Used to describe a legal entity, which submits data into or extracts data from the ghTrack service.
ghTrack	Data-as-a-service with multiple service modules.
GSH	General Security Handbook - Security handbook for GateHouse employees for handling general security related issues; not for public distribution.
May	Used to describe a permissible way to achieve compliance.
PII	Personal Identifiable Information – this also includes positional information, license plates etc.
PQM	Process & Quality Management – GateHouse's quality management system certified according to DS/EN ISO 9001:2008[2]; not for public distribution.
Shall or must	Compliance is mandatory.
Should	Compliance is recommended, but not mandatory.

[1] http://www.gatehouse.dk/logistics/

[2] GateHouse is DS/EN ISO 9001:2008 certified for the following product or service ranges: **"Development of customer specific software solutions. Service provision, support and maintenance of mission critical communication systems. Consultancy within communication systems and equipment."**

User	Used to describe a person which has a user profile on the ghTrack service.

Security Statement

1 GateHouse Policies and Procedures

1.1 Information Security Management

GateHouse Logistics A/S has a GSH which state how information security shall be managed within GateHouse Logistics A/S. This covers not only general internal information security, but product and service specific information security as well, such as those regarding the ghTrack service and ghTrack's customers and users.

The GSH specifies how all employees should conform to information security and data management for customers/users, and is influenced by the FKOBST 358-1[3].

1.2 Human Resources and Education

All personnel that have access to, or administrate production environments, which contain PII, are educated in the concepts of information security and relevant technologies and must adhere to all relevant security processes within GateHouse Logistics A/S. Only employees who have been certified by GateHouse COO can gain access to perform administrative operations on production environments for ghTrack. This however, does not enable employees to gain direct access to any PII.

1.3 Access Control

Access to any security critical part of the ghTrack service backend, such as databases, backup or other production environments, are only provided to specific employees on a need-to-know basis. Access to each of these systems is handled in coherence with the internal information security management according to GSH.

1.4 Production Monitoring

All production systems and servers are monitored for malicious activity and maintained accordingly – both manually and via automatic monitoring. Access logs to servers, and production service environments are reviewed accordingly.

[3] https://fe-ddis.dk/SiteCollectionDocuments/FE/Militaersikkerhed/FKOBST358-1.pdf

1.5 Design and Development Standards

ghTrack is designed and developed in conformance with our PQM, which is DS/EN ISO 9001:2008 certified and is influenced by CMMI L3.

1.6 ghTrack Development Stack

ghTrack is primarily coded in C++, Java, JavaScript and PostgreSQL. Application and database management systems run on a mix of Linux and Windows servers. Furthermore, ghTrack utilize managed cloud services.

1.7 Coding Standards

Development and software programming is performed according to GateHouse Logistics A/S internal PQM approved development standards and source code style guide. All production code is subject to regular code inspection/review and testing.

2 Hosting Services and Data Policy

2.1 Hosting Service Provider

GateHouse Logistics A/S uses one or several cloud service provider(s) for the ghTrack service. Such cloud service provider(s) are bound by a data controller privacy policy agreement with GateHouse Logistics A/S, which prohibits the cloud service provider(s) to observe, or provide, any information or data in relation to ghTrack to third parties.

2.2 Infrastructure

All data, and production environments for ghTrack are stored and hosted on GateHouse Logistics A/S's private and secure cloud services within the cloud service partner(s) server. No third party has access to any data on GateHouse Logistics A/S hosting services.

2.3 No-Direct-Data Access Policy

GateHouse Logistics A/S has designed ghTrack to adhere to a "No-Direct-Data Access Policy". This means that ghTrack cannot be used by GateHouse Logistics A/S administrative staff, in any way, to access any customer PII data. This includes e.g. direct database queries, direct backend access, or frontend manipulation. In any case, data owner is always responsible for giving permission to those

customers who should be able to view/access their data, which can only be done via the ghTrack service itself.

2.4 Data Access in Case of Unforeseeable Events

As long as GateHouse Logistics A/S has legal ownership of ghTrack and its production environments and hosting services, ghTrack customers shall be able to access their data via the ghTrack service. Only upon special requests can data be acquired directly from GateHouse Logistics A/S, i.e. if data cannot be acquired from ghTrack.

In the case where GateHouse Logistics A/S is no longer an established legal identity, or a business organization of any sort which allows GateHouse Logistics A/S to maintain or withhold ghTrack and its data as described within this document and ghTrack license agreements GateHouse Logistics A/S will release a formal notice to all ghTrack users to inform them of the specific circumstances and why they have unfolded.

However, these procedures do not unfold if another legal identity accepts, or overtakes the legal data responsibilities of GateHouse Logistics A/S in regards to ghTrack and its customer's data – in this case, all ghTrack customers will be informed beforehand.

2.5 Hosting Service Security Certificates and Standards

GateHouse Logistics A/S only uses professional cloud service partners certified under international and industry-specific standards such as: ISO:27001, ISO 27017, ISO 27018, ISO 9001:2015, C5 (DE), and Cyber Essentials Plus (UK).

2.6 ghTrack Data and Hosting Location

All data in relation to ghTrack is stored on secured hardware located within the EU. GateHouse Logistics A/S highly values its customers' data privacy and security, and therefore highlights that information such as a physical street address or housing of data servers is non-relevant in this case of data privacy and security and will only be regarded as a security-risk if revealed.

Due to the fact that GateHouse Logistics A/S is a legal identity within the kingdom of Denmark, GateHouse Logistics A/S must conform to Danish and EU laws and regulations regarding data privacy and data control, hereunder the Danish Act on Processing of Personal Data[4]. According to both the Danish Data Protection Agency (Datatilsynet)[5] and the Danish Act on Security and

[4] https://www.datatilsynet.dk/english/the-act-on-processing-of-personal-data/read-the-act-on-processing-of-personal-data/compiled-version-of-the-act-on-processing-of-personal-data/

[5] Danish Data Protection Agency, please see http://www.datatilsynet.dk/

Protection of PII, which are handled by public legal identities (Sikkerhedsbekendtgørelsen)[6], it is NOT required by data controllers/processors such as GateHouse Logistics A/S to reveal more detailed information of physical addresses of data service providers and data servers, other than country or city/state specifics.

3 System Availability

3.1 Service and/or Database Failure

ghTrack makes use of multiple services to serve/store data to/from customers, such that if any server becomes unavailable the system will be able to operate without inconvenience or any loss of data.

3.2 Data Backup

Backup of data stored in databases is performed regularly such that data can be restored in case of any critical failures. Backup is performed by multiple machines, where data is continuously replicated multiple times 24/7/365. In addition, continuous file system backups are made on all data and stored separately. All backup data, and backup to any services used by ghTrack is kept within the geographical location of the EU.

3.3 Server Failure

If a server becomes unavailable, the ghTrack personnel is immediately notified such that a resolution can be found as quickly as possible. Server failures should not affect performance of the ghTrack service and users should in most cases not be affected by any server failures – see 3.1 and 3.2.

4 Infrastructure Security

4.1 Threat Management

GateHouse Logistics A/S's cloud service partner(s) provides threat management in relation to hosted services, and as such ghTrack and the underlying network used to link ghTrack services together is subject to threat management.

[6] Danish Act no. 528 since 15/06/2000 with changes (no. 201 since 22/03/2001) – Sikkerhedsbekendtgørelsen, please see https://www.retsinformation.dk/forms/r0710.aspx?id=842

4.2 Network Connection

The servers running ghTrack services are locked on all ports except for the ones used by the system internally, and only accepts requests from the internal service IP addresses. The public web-interface servers only accept connections on port 443 (HTTPS) and port 80 (HTTP), however access on HTTP shall always redirect to HTTPS in order to ensure full network encryption between all services and ghTrack customers and users.

4.3 Segregation of Testing Environment

All new system functionality and design changes are verified and validated according to GateHouse Logistics A/S PQM in a separate testing environment fully separated from the actual ghTrack production environment before being made available to the public production environments.

4.4 Release of New Versions

For every new ghTrack version rollout, all users of ghTrack are informed of the specifics and the time and date when a new release shall be rolled out. In most cases, a version rollout should not affect users in critical ways. If such critical releases are required, all users will be informed of the specifics timely, in order to prepare for any inconvenience which, they might experience.

4.5 Logging, Monitoring, and Reporting

Access to any services hosted by GateHouse Logistics A/S's cloud service partner(s) is subject to audit logging and as such all attempts to access any servers used by ghTrack are logged for security analysis and monitoring. Any server failure is automatically reported to the ghTrack operational personnel as well.

5 ghTrack Operation and User Security

5.1 Communication Encryption

All communication between users of ghTrack and the ghTrack service itself is encrypted with use of the Secure Socket Layer (SSL) and Transport Layer Security (TLS) technologies, which ensures that ALL data sent between users and the ghTrack service is obscured from outside parties. Furthermore, SSL and TLS makes use of data encryption and server verification, which implies that data only can be interpreted by the intended parties. The ghTrack system is split into different entities to ensure availability. All communication between the internal entities of ghTrack is performed via secure connections as well, such that data may not be interpreted by third parties during internal system

communication. All encryption standard for ghTrack, for both communication and data encryption, is at minimum AES-256 (i.e. the AES algorithm using 256 bit keys).

5.2 General User Security

In order to collect and view data, users must create a user account with an associated strong password, which shall be used to authenticate with the service. Users shall provide at least the following information and accept our usage terms before being able to authenticate against ghTrack.

- Full Name
- Username
- Password
- E-mail address
- Company CVR

User name to login is used as a unique identifier for user profiles. User sessions will in special cases timeout and must be reestablished by the user.

5.3 Authentication

To access any data through the API (DaaS), a user must be authenticated by an API key auto-generated by ghTrack.

5.4 User Password Standard

ghTrack requires user passwords to conform to a high level of password security to limit the possibility of brute-force attacks. Passwords cannot be recovered in clear text and do require users to create new passwords in case of a lost password. ghTrack's password policy is strict, and every user must define a password which comply with the following rules:

1. Eight characters long
2. One upper and one lower case character
3. One number
4. One special character

5.5 Password Protection Policy

Even though security measures are employed with regards to passwords, users are still responsible for defining their own secure passwords, and not sharing their passwords with anyone. GateHouse Logistics A/S recommends that individual organizations confirm with the ISO/IEC 27001/27002

standard, regarding information security management. ghTrack does not require users to change their passwords, but as a recommendation they should be changed regularly for security measures.

5.6 Access Logging

All non-successful authentication and unauthorized requests tries are logged within the system and are only accessible by ghTrack system administrators. These access logs are reviewed regularly as described in 1.4. If suspicious activity is noted, the specific user profiles will be analyzed in detail and the owner of the user profile will be contacted and/or the account will be deleted.

5.7 Audit and Transaction Logging

All critical actions performed by users of ghTrack are logged both in relation to general operations (e.g. user creation/edit) and data specific operations. Audit logging ensures that all operations performed by users can be traced. The audit/transaction logs contain information about the following:

1. User which performed the operation
2. Time/date of operation
3. What information was changed or which operation was performed
4. Old information values (if applicable)
5. New information values (if applicable)

System specific logs are kept indefinitely and always accessible by ghTrack administrative staff.

5.8 Deletion of Data

Telematics data and its logs are kept in memory for 14 days and hereafter deleted. Only data constituting a specific tour or data from equipment explicitly tagged as permanent tracked is stored within ghTrack and forwarded to customers according to the data sharing agreements between the data provider and GateHouse.

Stored telematics data and its logs are securely kept for a period of 180 days within ghTrack, unless specific considerations requires otherwise. The data owner can explicitly request for data deletion (database deletion). The data owner is always entitled to database deletion unless such deletion is prohibited by applicable law or by an agreement.

When a data owner requests for data to be deleted, ghTrack registers a "delete date" - which shall be no later than 10 days after delete request is made. After 10 days, the data is deleted completely from all ghTrack production services and the data owner is informed of successful deletion. Any

backups of the data are kept for maximum 7 days after the data has been deleted (see why in 3.3). Afterwards, data cannot be recovered in ANY way. GateHouse Logistics A/S has verified and validated this deletion method.

6 Breach of Security

GateHouse Logistics A/S incorporates the newest technologies for secure computing and data storage in cooperation with cloud service partners. However, data transmission over the internet and data storage can never be guaranteed 100% secure. As such, if a security breach should occur, the affected customers/users of ghTrack will be informed via personal e-mail sent to each individual customer/user. If customers do not respond to this formal notice within 3 calendar days, contact will be taken via telephone. A formal notice will contain the type of security breach the system was subject to and what measures have been taken to ensure minimal data breach. In addition, GateHouse Logistics A/S will inform all users of which actions to take to minimize any risk of inconvenience. All security breach incidents are reported and documented in a standardized way, as described in GateHouse Logistics A/S internal security management procedures, GSH.

Missing Information?

If you have any questions regarding security, data privacy, or technical documentation, you are always welcome to contact us via: support@gatehouse.dk