TransFollow platform security

Users of the TransFollow platform who enter consignment notes or shipment reports provide important company information. This information should only be visible to authorised persons. This document explains the measures that have been taken to ensure the security of the system and your data. It covers issues such as which standards and procedures are applied in TransFollow, which agreements TransFollow has reached with suppliers and how TransFollow monitors access to the system. Aspects such as availability and quality of the organisation and legislation are also discussed.

1. Introduction

The TransFollow platform allows users to securely and reliably prepare, send, modify and consult consignment notes or shipment reports. Important data protection measures include:

- access management;
- physical protection of the servers in the data centre;
- safeguarding continuity;
- general security of the application;
- short life-cycle of consignment notes and shipment reports.

The organisation that manages TransFollow has also been set out in accordance with ISO 27001. The legal reliability of the system has been examined for compliance with legislation and regulations on consignment notes and electronic transactions.

2. Data security

Security of data access

The data access (registration data, consignment notes, shipment reports) is linked to the user's account. Only the user can determine which other users can consult or modify the data. The TransFollow platform limits the possibility to modify the consignment notes. Once a user (sender, carrier or consignee) has signed the note, it can no longer be modified by that user.

All data from the platform is saved on the servers of a *hosting* company. An agreement has been made with the hosting company that the TransFollow platform is only accessible to customers with a TransFollow account. Procedural agreements have been reached for emergencies whereby the hosting company can only be granted access to the environment, the application and the data in cooperation with TransFollow B.V.

The data is not accessible to third parties.

Signature security

Passwords and signatures are protected with encryption algorithms and advanced key management so that hacking is virtually impossible. With this protection, TransFollow prevents data leaks to unauthorised persons.

Physical security

TransFollow is hosted by an enterprise hosting party in a secured and redundant environment. According to our policy, suppliers of critical and secured environments including the hosting party, have to comply with the necessary certifications, such as ISO 27001.

The security of the servers on which all TransFollow data is stored has been laid down in legal terms in a Service Level Agreement (SLA) with the hosting party. The provisions of the SLA include emergency measures for the data centres in case of power source fail. Evidently the server rooms are cooled in accordance with the requirements stipulated by the fire service. Access to the buildings in which the servers are housed is only possible when the access procedure is properly met. Finally, the TransFollow platform uses two different locations for the servers. These locations will always be at least five kilometres apart.

All our systems are carried out redundantly in varying layers (physical and virtual). This ensures the availability of our systems. By using 24/7 monitoring and management, malfunctions in the platform are automatically detected and can be solved directly.

Availability

As logistics processes continue day and night, TransFollow needs to be available 24/7. Thanks to a set of redundant systems, back-up plans and monitoring, the risk of systemfailure is kept to a minimum. The software supports various off-line scenarios (i.e. when there is no internet connection) for the electronic signature, including the possibility to sign on screen (‘sign-on-glass’). The use of TransFollow can fluctuate considerably and can therefore influence the availability (such as performance). The flexibility of the hosting infrastructure means that it can be upscaled very quickly if needed, thereby guaranteeing availability.

In order to timely identify security risks, both the individual components, the platform and the system are monitored and analysed. Specific procedures have been put in place to ensure follow-up in case of problems and calamities.

Application security and audits

During the TransFollow development phase, attention was constantly paid to the security of the application and the data. Both before and during the development process, the application was continuously tested against extensive quality criteria, including those from the NCSC “ICT-Beveiligingsrichtlijnen voor Webapplicaties, the focus being on reliability, usability, compatibility,

efficiency, maintainability and portability. The risk of code abuse has been further minimised by testing all components both individually and as an integral system.

The TransFollow data model has been designed for security and reliability, since for operational management purposes users must be able to rely on the availability of their consignment notes and shipment reports. Data entry validation, integrity checks and detailed log mechanisms have been built into the application. TransFollow uses proven communication standards that keep the risk of data loss to a minimum.

These communication standards are tested for proper implementation. ISO 27002 requires an annual audit. The software was also checked several times by means of code reviews during the development phase. Finally, a specialised firm carries out software penetration tests (hacker tests).

Data security

The life cycle of the data in the TransFollow platform has been clearly defined. Data from consignment notes and shipment reports will be kept for a maximum of two weeks. The data are destroyed in such a way that reproduction is impossible. Data ownership has been clearly defined and technical procedures are in place to ensure that no data can be copied between environments and networks. The procedures for access to the production data are limited extensively, therefore also TransFollow does not have access.

From a user perspective it may be necessary to retain data longer. We therefore advise customers to store their data (e.g. the TransFollow consignment note) on their own systems for at least one year, but preferably for seven years. TransFollow will enable companies to do this by providing sealed PDF files (certified) to the parties. This means that if a claim is made for damages, the party concerned can show the sealed PDF file to the insurance company as proof. The consignment note is sealed immediately after the recipient has placed any optional comments and has signed for reception. Once the note has been sealed, the parties have two weeks to download the sealed PDF file. Customers can also opt to archive data at TransFollow. The consignment notes will then be stored in the TransFollow archive for a period of seven years (for a fee). The security measures that are taken for the archive correspond to the security measures taken for the rest of the TransFollow platform. The archive is managed by the same hosting party.

Independent data manager

TransFollow B.V., as the owner of the TransFollow platform, is an independent organisation. TransFollow B.V. aims to facilitate the logistics chain by exchanging and storing data on logistics transactions. The TransFollow platform has been developed for this purpose. Security and reliability have been the main focus with regards to both the development and the management of TransFollow. TransFollow B.V. sees this as its responsibility in the interests of the logistics industry. It considers the use of data for other purposes as highly undesirable. The shielding and destruction of outdated data has therefore a high priority, technically, operationally and contractually.

3. Management and organisation

Many companies and organisations are involved in the development and management of the TransFollow platform. TransFollow B.V. sets stringent requirements in terms of its own internal processes and those of its partners. TransFollow B.V. is ISO 27001 certified and therefore complies with international information security guidelines. TransFollow is managed in an organisation that has established processes for modifications, software testing and the distribution of the software to end-users. The separation of responsibilities is clearly defined within these processes. Testing takes place on the basis of a planning and control cycle. Moreover, regular risk analyses are carried out by TransFollow B.V. on vulnerable parts of the processes.

Functional modifications of the platform have to be approved by a Change Advisory Board, which includes representatives of all parties concerned. Modifications are taken into production by means of a strictly defined release management process. Here again, representatives of various parties are involved.

4. Legislation

We have identified the following legislation to which the TransFollow platform has to comply:

- Legislation on consignment notes;
- Legislation on electronic transactions, including electronic signatures;
- Legislation on the protection of personal data.

The requirements have been formulated together with legal experts specialised in transport law and ICT law. The TransFollow platform fully complies with these requirements.

TransFollow data are stored with a Dutch hosting company that uses data centres established in the Netherlands. This means that Dutch law applies.

5. Finally

If you have any further questions about TransFollow security, please contact the supportdesk of TransFollow B.V. on 088-55 22 122.