Systems acquisition, development & maintenance

As a software company, the security and reliability of all of our products depend on secure coding principles and processes to ensure an agile product life cycle.

Our Secure Software Development Lifecycle includes:

- Peer reviewed design and coding
- Style guidelines
- QA functional / load testing
- Release and Change Management
- Static code reviews (OWASP Top 10 / SANS Top 25)

In addition, we facilitate the following programmes to secure our engineering perimeter:

- Security education for our work force
- Implementation-level security testing and review
- System hardening
- Vulnerability / patch management
- Web-Application-Security testing

Engineering

Software design analysis

Completed development

Static inspection of code

Quality assurance

Dynamic analysis of the application

Deployment

Deployment and stabilisation of the application

Let's drive business

www.tomtom.com/telematics

Supplier relationships

Managing external threats on the edge of our scope helps to ensure, that no additional risks are added to the organisation through our partner or supplier relationships. When possible, we select suppliers who maintain an international compliance standard for information security, and/or adhere to similar values as TomTom related to the protection of information and data privacy.

Information security incident management

Should a security incident occur, it is important to have an effective approach for managing the incident. This includes the timely communication to all interested parties, and reporting of internal security weaknesses to support a secure perimeter as dictated by the various legislative, regulatory and contractual agreements in place for notification.

Information security aspects of business continuity management

We manage a detailed business and information security continuity programme to ensure that the TomTom Telematics Service Platform will be available to our customers even in the event of a disaster. Through our active/active data centre configuration, the probability of a major disaster in both centres is unlikely as each centre can maintain our entire operation if necessary. This means you can rely on the platform being available when you need it.

COMPLIANCE AND DATA PRIVACY

TomTom Telematics is controlled and audited through our Data Privacy Officer (DPO) to ensure compliance with the EU General Data Protection Regulation as well as other relevant local privacy legislations.

Our Information Security Management System (ISMS) team performs regular reviews of legal or security requirements which might have an effect on our telematics platform or the informational assets in scope of the ISMS.

HIGHLIGHTS

- **MAXIMUM SECURITY AND INTEGRITY**
  Your data is in safe hands with our ISO 27001 certified system.
- **PROTECTING DRIVER PRIVACY**
  WIth our focus on data protection, we have worked together with data privacy groups and work councils to demonstrate our commitment to your privacy.
- **DATA DELETION**
  Data is marked as dereferenced and overwritten in the event of data deletion to prevent data from being recovered by unauthorised parties.
- **DATA RETENTION**
  Per default, we retain all detailed data including precise data tracks for up to ninety (90) days, and current year plus previous two (2) years for our logbook, dashboard and reporting. This may differ due to specific country related regulations.
- **CHOOSE INTEGRITY. PROTECT THE ENVIRONMENT**
  We do our part to provide you a secure platform, which allows you to save costs while doing your part for the environment.

TOMTOM TELEMATICS

Are you interested in more detailed technical information related to security and data privacy? The Certified Information Security and Data Privacy Telematics whitepaper may be requested from the TomTom Telematics website at **https://telematics.tomtom.com/isms**

Contact us:
privacy@telematics.tomtom.com

CERTIFIED INFORMATION SECURITY AND DATA PRIVACY TELEMATICS

TOMTOM TELEMATICS

AT TOMTOM TELEMATICS, WE'RE COMMITTED TO THE SECURITY OF INFORMATION AND DATA PRIVACY.

We invest continuously in our engineering, proven technologies, processes and people to ensure that we can always provide the most reliable telematics service platform on the market.

THE POWER OF TOMTOM TELEMATICS SERVICE PLATFORM

ISO/IEC 27001:2013 INFORMATION SECURITY CERTIFIED
Our service platform and our mature processes have been certified ensuring that our customers benefit from the highest level of protection for information security and data privacy.

HIGHEST STANDARD EV SSL ENCRYPTION
Secure, encrypted login and data transfer to our service platform. You can trust your data is safe and secure

LOCAL INSTALLATION
Nationwide and international installers

FIRST CLASS SUPPORT
From local resellers and system integrators

APP CENTER
Proven integrations and add-on apps available in the App Center

Let's drive business

www.tomtom.com/telematics

It's no surprise we're a global leader in fleet management and telematics.

As one of the world's largest providers of telematics services, continual improvement in our service is important to make sure that we are the best partner for your business – now and in the future.

ISO 27001 certified scope

Our Information Security Management System (ISMS) covers all of our critical business processes necessary to secure the informational assets related to the TomTom Telematics Service Platform. This includes the architecture, engineering, quality assurance and IT services provided to the TomTom Telematics B.V at our Technology Headquarters in Germany, as well as our secure data center co-locations located within the European Union. This is in accordance with the ISO/IEC 27001:2013 standard and implemented as detailed in our Statement of Applicability version from November 2016.

"The ISO 27001 certification underpins that we're in complete control of our processes and even more importantly, that our client data is in safe hands, which is crucial for us providing a business critical fleet management "Software as a Service (SaaS) solution."

Thomas Schmidt, Managing Director, TomTom Telematics

Information security management system

The cornerstone of TomTom Telematics' commitment to information security is our set of security policies and programmes which cover the organisation and management of information security. Based on our rigorous risk management programme aligned with our corporate objectives, a well-defined security perimeter is operated within the scope of the ISMS which includes, but is not limited to the following topics:

INFORMATION SECURITY POLICIES
A detailed set of security policies designed to provide management direction and support of the information management system and all operational activities with respect to the TomTom Telematics Service Platform.

ORGANISATION OF INFORMATION SECURITY
Information security is everyone's business.
The roles and responsibilities of all employees are based on information security. Together with a full-time information security team, everyone ensures compliance and governance to the ISO 27001 as well as alignment to the EU General Data Protection Regulation (GDPR), as well as all relevant local privacy legislations.

HUMAN RESOURCES SECURITY
Information security is crucial prior to, during, and after the termination of employment. This includes selecting the right employees and providing them continual customised training.

ASSET MANAGEMENT
Inventory, ownership and maintenance throughout the asset life-cycle, ensures proper categorisation, labelling and risk owner assignment. This includes the secure handling of company intellectual property and customer data.

ACCESS CONTROL
Through identity management, all access is limited to a need-to-have and a need-to-know basis. Additional controls assist to prevent unauthorized access. For example, system logging and monitoring provide real-time detection across our security perimeter.

CRYPTOGRAPHY
We invest in state-of-the-art hardware and software solutions. Proven cryptographic technologies protect the confidentiality and integrity of our customer's data and our operational systems.

PHYSICAL AND ENVIRONMENTAL SECURITY
We operate two independent Tier3+ data centres within the European Union due to its strict data privacy requirements. Our proven active/active configuration ensures disaster recovery and high availability capabilities which are tested regularly.

OPERATIONAL SECURITY
We strive to maintain a managed, strict and repeatable process within our operations. By establishing security baselines, risk levels are managed and allow for efficient operational execution.

Operational security highlights:
- **Operational procedures and documentation**
- **Backup / Restore tests of critical systems**
- **Monitoring of operational environments**
- **Incident, Problem and Change-Management based on best practices**
- **Capacity Management including load testing**
- **Segregation of duties**
- **System hardening**
- **Separation of environments for development, testing, and production**
- **Vulnerability scanning**
- **Penetration testing**
- **Patch management**

COMMUNICATIONS SECURITY
Security of data while "in-transit" requires a secure network through which to travel. We employ secure methods of communication such as:

- **Network segregation**
- **VLAN separation, DMZ with multi-level Firewalls**
- **Network Access Controls (NAC)**
- **Encryption per default using latest industry standards**

TOMTOM TELEMATICS