Kauf, Entwicklung und Wartung von Systemen

Für uns als Softwareunternehmen erfordert die Sicherheit und Verlässlichkeit all unserer Produkte sichere Programmierungsrichtlinien und -prozesse, um einen agilen Produktlebenszyklus zu gewährleisten.

Unser SSDLC (Secure Software Development Life Cycle) umfasst folgende Punkte:

- Überprüfung des Designs und der Programmierung nach dem Vier-Augen-Prinzip
- Gestaltungsrichtlinien
- Qualitätsfunktions-/Belastungstests
- Freigabe- und Change Management
- Prüfung von statischem Programmcode (OWASP Top 10/ SANS Top 25)

Darüber hinaus schützen wir unsere Engineering-Umgebung mit den folgenden Schritten:

- Sicherheitsausbildung unserer Mitarbeiter
- Sicherheitstests und -prüfungen auf Implementierungsebene
- Systemabhärtung
- Management von Sicherheitsrisiken/Patches
- Webanwendungssicherheitstests

010101
001010

Engineering	Abgeschlossene Entwicklung	Qualitäts-sicherung	Bereitstellung
Software Design Analyse	Statische Prüfung von Code	Dynamische Analyse der Anwendung	Bereitstellung und Stabilisierung der Anwendung

Let's drive business®

www.tomtom.com/telematics

Lieferantenbeziehungen

Um uns gegen externe Risiken am Rande unseres Wirkungsbereiches abzusichern, stellen wir sicher, dass unsere Partner oder Lieferanten kein zusätzliches Risiko für unser Unternehmen darstellen. Wenn möglich, wählen wir Lieferanten, welche die internationalen Compliance-Standards für Informationssicherheit einhalten und/ oder ähnliche Werte wie TomTom bezüglich Datenschutz vertreten.

Vorfallsmanagement in der Informationssicherheit

Bei einem Sicherheitsvorfall ist ein effektiver Ansatz zur Vorfallshandhabung entscheidend. Dieser umfasst die schnelle Benachrichtigung aller betroffenen Parteien sowie die interne Meldung von Sicherheitslücken, um eine sichere Umgebung zu schaffen, wie es durch die verschiedenen bestehenden rechtlichen, regulatorischen und vertraglichen Vereinbarungen zur Benachrichtigung vorgegeben ist.

Informationssicherheit beim betrieblichen Kontinuitätsmanagement

Wir verfügen über ein umfassendes Programm zur fortlaufenden Geschäfts- und Informationssicherheit, um sicherzustellen, dass die TomTom Telematics-Dienstplattform unseren Kunden auch in einem Notfall durchgehend zur Verfügung steht. Dank unserer Aktiv/ Aktiv-Rechenzentrumskonfiguration kann jedes Zentrum bei einem Notfall im anderen Zentrum den gesamten Betrieb alleine übernehmen. So können Sie beruhigt darauf vertrauen, dass unsere Plattform verfügbar ist, wenn Sie sie brauchen.

COMPLIANCE UND DATENSCHUTZ

TomTom Telematics wird durch unseren Datenschutzbeauftragten kontrolliert und geprüft, um sicherzustellen, dass die EU-Datenschutz-Grundverordnung (EU-DSGVO) und andere relevante lokale Datenschutzbestimmungen eingehalten werden.

Unser Information Security Management System (ISMS)-Team führt regelmäßige Prüfungen von rechtlichen und sicherheitstechnischen Anforderungen durch, die einen Einfluss auf unsere Telematikplattform oder die Informationsbestände im Rahmen des ISMS haben könnten.

HIGHLIGHTS

- **MAXIMALE SICHERHEIT UND INTEGRITÄT**
  Ihre Daten sind mit unserem ISO 27001-zertifizierten System in sicheren Händen.
- **SCHUTZ DER FAHRERPRIVATSPHÄRE**
  Im Rahmen unserer Bemühungen zum Thema Datenschutz haben wir eng mit Datenschutzgruppen und Betriebsräten zusammengearbeitet, um unser Engagement für Ihre Privatsphäre in die Tat umzusetzen.
- **DATENLÖSCHUNG**
  Bei einer Datenlöschung werden die Daten als dereferenziert markiert und überschrieben, um die Datenwiederherstellung durch andere Parteien zu vermeiden.
- **DATENAUFBEWAHRUNG**
  Standardmäßig bewahren wir alle Daten, darunter präzise Datenspuren, bis zu neunzig (90) Tage und unsere Fahrtenbuch-, Dashboard- und Reportingdaten über das aktuelle Jahr plus zwei (2) weitere Jahre auf. Dies kann aufgrund der jeweiligen länderspezifischen Bestimmungen abweichen.
- **ENTSCHEIDEN SIE SICH FÜR INTEGRITÄT. SCHÜTZEN SIE DIE UMWELT.**
  Wir leisten unseren Beitrag, um Ihnen eine sichere Plattform bereitzustellen, mit der Sie Kosten sparen und Ihren Beitrag zum Umweltschutz leisten können.

TOMTOM TELEMATICS

Sie wünschen detailliertere technische Informationen zum Thema Sicherheit und Datenschutz? Dann fordern Sie das Whitepaper „Certified Information Security and Data Privacy Telematics" auf der TomTom Telematics-Website an:
https://telematics.tomtom.com/isms

Kontaktieren Sie uns:
privacy@telematics.tomtom.com

TELEMATIK MIT ZERTIFIZIERTER INFORMATIONSSICHERHEIT UND ZERTIFIZIERTEM DATENSCHUTZ

TOMTOM TELEMATICS

WIR BEI TOMTOM TELEMATICS FÜHLEN UNS DER INFORMATIONSSICHERHEIT UND DEM DATENSCHUTZ VERPFLICHTET.

Daher investieren wir fortlaufend in unser Engineering, bewährte Technologien, Prozesse und Mitarbeiter. So können wir jederzeit die zuverlässigste Serviceplattform der gesamten Branche im Bereich Telematik bereitstellen.

DIE LEISTUNGSFÄHIGKEIT DER TOMTOM TELEMATICS-SERVICEPLATTFORM

INFORMATIONSSICHERHEIT NACH ISO/IEC 27001:2013
Unsere Serviceplattform und unsere ausgereiften Prozesse wurden dafür zertifiziert, dass sie unseren Kunden das höchste Maß an Informationssicherheit und Datenschutz garantieren

EV-SSL-VERSCHLÜSSELUNG NACH HÖCHSTEN STANDARDS
Sichere, verschlüsselte Anmeldung und Datenübertragung an unsere Serviceplattform. Sie können darauf vertrauen, dass Ihre Daten jederzeit geschützt sind

LOKALE INSTALLATION
Nationale und internationale Installationsdienste

ERSTKLASSIGER SUPPORT
Von lokalen Händlern und Systemintegratoren

APP CENTER
Bewährte Integrationen und App-Erweiterungen im App Center

Es ist kein Geheimnis, dass wir ein weltweiter Marktführer in den Bereichen Flottenmanagement und Telematik sind.

Als einer der größten Anbieter von Telematikdiensten ist eine fortlaufende Verbesserung unserer Dienste wichtig, um sicherzustellen, dass wir der beste Partner für Ihr Unternehmen sind – jetzt und in Zukunft.

Umfang der ISO 27001-Zertifizierung

Unser Information Security Management System (ISMS) umfasst sämtliche kritische Unternehmensprozesse, um die Informationsbestände bezüglich der TomTom Telematics-Serviceplattform zu sichern. Dies umfasst Architektur-, Engineering-, Qualitätssicherungs- und IT-Dienste, die TomTom Telematics B.V. in unseren Technology Headquarters in Deutschland und unseren sicheren Rechenzentrumsstandorten in der EU zur Verfügung gestellt werden. Dies geschieht unter Einhaltung des ISO/IEC 27001:2013 Standards. Die Implementierung erfolgt dabei gemäß unserer Erklärung zur Anwendbarkeit, Stand November 2016.

„Die Zertifizierung nach ISO 27001 verdeutlicht, dass wir unsere Prozesse fest unter Kontrolle haben. Zudem können wir so belegen, dass die Daten unserer Kunden in sicheren Händen sind, was für die Bereitstellung einer geschäftskritischen SaaS-Lösung (Software-as-a-Service) entscheidend ist.“

Thomas Schmidt, Managing Director, TomTom Telematics

Information Security Management System

Der Schutz von Informationen durch TomTom Telematics basiert auf einer Reihe von Sicherheitsrichtlinien und -programmen, die die Organisation und das Management der Informationssicherheit abdecken. Basierend auf unserem strengen Risikomanagementprogramm und in Übereinstimmung mit unseren Unternehmenszielen findet ein genau definierter Sicherheitsperimeter im Rahmen des ISMS Anwendung, welcher unter anderem folgende Bereiche abdeckt:

RICHTLINIEN FÜR DIE INFORMATIONSSICHERHEIT
Eine detaillierte Zusammenstellung von Sicherheitsrichtlinien erlaubt eine Richtungsvorgabe zur Steuerung sowie die Unterstützung des Informationsmanagementsystems und aller betrieblichen Vorgänge im Zusammenhang mit der TomTom Telematics-Serviceplattform.

ORGANISATION DER INFORMATIONSSICHERHEIT
Informationssicherheit geht uns alle an.
Die Rollen und Verantwortlichkeiten aller Mitarbeiter basieren auf Informationssicherheit. In Zusammenarbeit mit einem in Vollzeit beschäftigten Informationssicherheitsteam gewährleisten alle Mitarbeiter die Einhaltung und Governance der ISO 27001-Richtlinien sowie der EU-Datenschutz-Grundverordnung (EU-DSGVO) und aller relevanten lokalen Datenschutzbestimmungen.

PERSONALSICHERHEIT
Informationssicherheit ist vor, während und nach Ende einer Beschäftigung entscheidend. Dies umfasst die Auswahl der richtigen Mitarbeiter und ihre fortlaufende, individuelle Weiterbildung.

ASSETMANAGEMENT
Die Inventarisierung, Verantwortlichkeitszuweisung und Pflege während des gesamten Assetlebenszyklus stellen die ordnungsgemäße Kategorisierung, Kennzeichnung und Zuordnung von Risikoeignern sicher. Dies beinhaltet den sicheren Umgang mit betriebseigenem geistigen Eigentum und Kundendaten.

ZUGRIFFSKONTROLLE
Durch Identitätsmanagement werden alle Zugriffe auf der Basis von „need-to-have" und "need-to-know" beschränkt. Der nicht autorisierte Zugriff wird zudem durch weitere Kontrollmechanismen verhindert. Beispielsweise bieten Systemprotokollierungs- und Überwachungsfunktionen eine Echtzeit-Erkennung über den gesamten Sicherheitsperimeter hinweg.

VERSCHLÜSSELUNG
Wir investieren in hochmoderne Hardware- und Software-lösungen. Bewährte Verschlüsselungstechnologien gewährleisten die Vertraulichkeit und Integrität unserer Kundendaten sowie Betriebssysteme.

PHYSISCHE UND UMGEBUNGSSICHERHEIT
Wir betreiben zwei unabhängige Tier3+-Rechenzentren in der EU, um die strengen Datenschutzbestimmungen zu erfüllen. Aufgrund der Aktiv/Aktiv-Konfiguration können wir eine vollständige Notfallwiederherstellung und eine optimale Verfügbarkeit gewährleisten, die regelmäßig getestet werden.

BETRIEBLICHE SICHERHEIT
Wir möchten einen gesteuerten, konsequenten und wiederholbaren Prozess für unsere betrieblichen Abläufe aufrechterhalten. Durch die Einführung von Sicherheitsrichtlinien werden Risikostufen gemanagt und dadurch eine effiziente operative Umsetzung erreicht.

Betriebliche Sicherheit – Highlights:

- **Betriebsabläufe und Dokumentation**
- **Backup-/Wiederherstellungs-Testläufe für wichtige Systeme**
- **Überwachung von Betriebsumgebungen**
- **Ereignis-, Problem- und Veränderungsmanagement basierend auf Best practices**
- **Kapazitätsmanagement, einschließlich Belastungstests**
- **Aufgabentrennung**
- **Systemabhärtung**
- **Trennung der Umgebungen für Entwicklung, Tests und Produktion**
- **Überprüfung von Sicherheitsrisiken**
- **Penetrationstests**
- **Patch Management**

KOMMUNIKATIONSSICHERHEIT
Die Sicherheit von verschickten Daten erfordert ein sicheres Netzwerk. Wir nutzen sichere Kommunikationsmethoden wie:

- **Netzwerkisolierung**
- **VLAN-Trennung, DMZ mit mehrstufigen Firewalls**
- **Netzwerkzugriffskontrollen (Network Access Controls, NAC)**
- **Standardmäßige Verschlüsselung nach den neuesten Industriestandards**