Information Security Annex

1. Scope and Principles

This Information Security Annex (hereafter: ISA), which includes information and IT security requirements must apply to Deliverables that are provided to TomTom by Supplier (hereafter: Supplier). These requirements are set as a minimum. These minimum requirements may not ensure an adequate level of information security when implemented on their own. The supplier is expected to exercise good judgement and provide secure Deliverables based on standard industry practices and good engineering principles and processes. The Supplier will ensure to meet all relevant legal and regulatory requirements including data protection, intellectual property rights and copyright. When applicable, TomTom will also share up front relevant additional information security policies with which the Supplier needs to comply. The requirements apply for the duration of the Deliverables provided, regardless of whether the Deliverables are procured with an Agreement or via third party distributors. Refer to section 12 for an overview of definitions of terms used in this ISA. Section 13 provides an overview with amendments for this specific Supplier

2. Contractual and Standards Compliance

Paragraph	
2.1	Security Policies The Supplier must define and implement an information security policy. The policy must be: • drafted according to the ISO/IEC 27001 standard or similar industry standard; • approved by top management and reviewed every two years; • adequate, relevant and effective; and • available to all employees and third parties.
2.2	Certification Where applicable, if the Supplier is information security certified (e.g. ISO/IEC 27001), the Supplier must: • provide TomTom with its information security certification(s); • keep TomTom informed of renewals or revocations of the certificate(s); and • maintain such certification during the entire term of the contractual duties.
2.3	Audit Where applicable and with prior written notice, TomTom or an appointed external party is entitled to, annually, perform audits to check Suppliers compliance with TomTom's information security requirements as defined in this ISA and any additional information security requirements set forth in the Agreement. If applicable, the Supplier will agree with a timely correction of relevant issues raised in the audit report.
2.4	Limitation of use of TomTom information The Supplier must use TomTom information transmitted, processed, generated and/or stored (in the XaaS/Cloud Service) only to provide the said Deliverables.
2.5	TomTom data reversibility (NOTE: only applicable where not addressed within the TomTom Terms and Conditions) Upon termination of the Agreement, the Supplier must make available to TomTom all TomTom data in a format and for a period of time mutually agreed between both parties Furthermore, the Supplier must irreversibly destroy all TomTom data in a manner designed to ensure that they cannot be accessed or read.

3. Security Organization

Paragraph	
3.1	Risk assessment and treatment The Supplier must have documented processes and routines for handling information security risks within its operations and when developing software, applications, application programming interfaces (“APIs”) or other content or engaging with all new third-party suppliers, partners and contractors related to the Deliverables. The Supplier must conduct at least once annually an information security audit of controls against standard industry practices. Where required, TomTom will request a report of the outcome.
3.2	Security point of contact The Supplier must nominate a point of contact for information security related matters. The point of contact must be provided to the TomTom business owner (main stakeholder of the Supplier) and changes must be communicated promptly.
3.3	Segregation of duties The Supplier must have a segregation of duties (including but not limited to a four-eye principle) process to prevent (an) individual(s) from controlling all key aspects of a critical transaction or business process. E.g. Developers should not be able to write code, perform testing and upload to production without a review.

4. Professionals and security

Paragraph	
4.1	Awareness training and education The Supplier must ensure that its employees appointed to provide the Deliverables: • possess appropriate Information security knowledge (e.g. managing security incidents and handling TomTom information); and • are familiar with the content and the implementation of applicable information security and privacy rules and procedures and the correct information processing requirements.
4.2	Screening The Supplier must perform relevant employee background checks to the extent permitted by applicable law and inform TomTom in case screening has not been completed or if the results give cause for doubt or concern.
4.3	Mobile devices The Supplier must ensure that TomTom information on mobile devices is managed and secured through a mobile device management (MDM) system. In the absence of an MDM system, no TomTom information will be stored on mobile devices.
4.4	Physical security of Suppliers facilities The Supplier must ensure that all its facilities, including but not limited to offices, data centers and warehouses, used for delivering content and other information and services to TomTom must include at least: • adequate perimeter and entry controls in line with local regulations and standards to ensure that only authorized personnel are allowed access; • visitors must be escorted and/or observed when on the premises; • a process must be in place to ensure all staff and visitors must return keys/cards when no longer needed; and

	• supplies received or sent on behalf of TomTom will be protected from theft, manipulation or destruction.

5. Access to and use of TomTom's assets (logical access)

Paragraph	
5.1	Granting of access to TomTom's systems and applications Where access is given to TomTom's systems and information (including remote access), the following will apply: • access will be provided on the principle of least privilege; • notify TomTom of any terminations or movement of staff, within a maximum of 7 working days (TomTom should be notified once an employee provides notice of resignation, once tasks has been completed or as soon as an employee departs the organization); and • all accounts must be used by the appointed individual only.
5.2	Integration with TomTom's resources and applications If Supplier resources are used to access and/or integrate with TomTom systems or applications, the Supplier must: • make sure that authentication is implemented using TomTom's authentication mechanism (e.g. Microsoft AD/ Azure); • ensure all user IDs are personal, uniquely identifiable and used only by the appointed individual. Each user ID must be both accountable and auditable; • implement a strong authentication system (Multi-Factor Authentication) for access to such resources; and • retain logs for the duration agreed in the Agreement including associated documents (e.g. Non-Disclosure Agreement or Data Processing Agreement) or 3 months by default.
5.3	Management of TomTom Resources Upon termination of the Agreement, the Supplier must return any and all TomTom resources still in its possession. Duplication of TomTom resources is also prohibited unless explicitly authorized.

6. Cryptography

Paragraph	
6.1	Encryption techniques The import, export and use of encryption techniques must be in compliance with applicable laws, regulations and standard industry practices. The following rules must apply when the Supplier stores or processes TomTom information: • all information must be encrypted at-rest. This includes information on mobile devices such as laptops, phones and other portable computing devices; • information must be encrypted-in-transit, at a minimum when it traverses the internet; • any wireless networks used must be encrypted; and • all non-console administrator access must be done over encrypted channels and in a secure way.

6.2	Key management The Supplier must ensure that keys and other secrets be stored in a secure way according to standard industry practices. In particular: • passwords should be stored using a modern password hashing function and a unique salt for each account; • encryption keys must only be distributed over secure channels; and • private and public keys generated for TomTom users must be unique and constitute a functioning key pair corresponding to digital certificates.
6.3	External certificate authority (CA) Where an external certificate authority (CA) is used by the Supplier, the CA must be accredited by a trustworthy party and the Supplier must provide TomTom with all details regarding the certificate and the CA. It is expected that the Supplier must act as the registration authority when an external CA is used.

7. Operations and Information systems

Paragraph	
7.1	Change management Any changes made to TomTom systems or applications must follow the TomTom change management process.
7.2	Capacity management Detective controls must be put in place to indicate and prevent problems related to capacity of all TomTom resources.
7.3	Production data and environments The Supplier must not use production data for testing activities. The Supplier must separate development, testing and production environments (e.g. networks, data, applications, etc.).
7.4	Patch management Supplier must keep resources up-to date with the latest information security patches and operating systems patches and installed software (including but not limited to anti-malware software).
7.5	Logging The Supplier must ensure that event logs, containing user activities, exceptions, faults and information security events are logged, kept for a minimum of 3 months and reviewed at least monthly. Information must be protected against unauthorized access.
7.6.	Operational software (NOTE: only applicable to Software Deliverables) • the Supplier must ensure that any software used to perform the services under the Agreement, is fully owned or licensed by the Supplier; • the modifications and changes to software and applications must be completed by authorized individuals; • where required operational systems must only hold approved executable code; • software provided by the Supplier must only be implemented in TomTom production environments after extensive and successful testing; • the Supplier shall provide TomTom with release notes, list the test executed, including the test results; • software bugs and the severity of the bugs found should also be provided to TomTom; • all software provided by the supplier must have version control, be retained as a contingency measure and all versions archived; • vendor support for software must be maintained throughout the duration of the Agreement; and

	TomTom must be notified before any change of a software version.
7.7	Security engineering principles Where the Supplier has no information security engineering principles, TomTom principles (TomTom policies and standards) must apply.

8. Vulnerability management

Paragraph	
8.1	Penetration tests Where TomTom information is stored in the Supplier network, the Supplier must conduct penetration tests at least on a yearly basis. It is expected that any critical findings where TomTom information is at risk, remediation efforts must be completed within at most 7 calendar days (CVSS v 3.0 score greater than 6).
8.2	Service level agreement to fix Vulnerabilities At a minimum, the Supplier shall scan infrastructure and applications for security vulnerabilities every 90 days. Furthermore, vulnerabilities found by the Supplier or reported by TomTom, impacting the Deliverables, must be scored according to the Common Vulnerability Scoring System ("CVSS") v3.0/ v4.0, and remediated within the time lines as detailed below. In case a vulnerability moves from "not actively being exploited" to "actively being exploited", the total number of remediation days must not exceed the numbers in column 3. **Table 1 Common Vulnerability Scoring System and remediation time lines**

Common Vulnerability Scoring System ("CVSS") v3.0/ v4.0	Remediation time lines of vulnerabilities "not actively being exploited"	Remediation time lines of vulnerabilities "actively being exploited"
3.9 score or lower	at best effort	at best effort
between 4 and 5.9	at most 90 calendar days	at most 30 calendar days
Any technical vulnerability with a CVSS score between 6 and 8.4	at most 30 calendar days	at most 7 calendar days
equal to or higher than 8.5	at most 7 calendar days	at most 48 hours

9. Network

Paragraph	
9.1	The Supplier must utilize standard industry practices to monitor, protect, safeguard and secure Deliverables and its services as well as TomTom's information, systems and network against unauthorized access, use and disclosure.
9.2	Where the Supplier provides network services, the Supplier must ensure the following: • limiting/ restricting access to network services and applications; • encrypting traffic between the network and internet; and • implementing network connection rules.
9.3	Where the Supplier network is being used by TomTom or where TomTom information is being stored or processed in the Supplier network, the Supplier must segregate its network.

10. Incident Management

Paragraph	
10.1	Notification The Supplier must notify TomTom in case of any information security incident, relating to the TomTom Deliverables and TomTom information within 24 hours from detection. TomTom may request a meeting to understand the root cause of the incident.
10.2	Resolution Upon notification of an incident, the Supplier and TomTom must agree on a resolution timeline (refer to 8.2 for incidents relating to vulnerabilities).
10.3	Suspension of Supplier access In the event of an information security incident which may impact TomTom, access to assets may be suspended by TomTom until the incident is resolved.
10.4	Legal In the event of legal action that involves or requires TomTom's information held or managed by the Supplier, the Supplier must cooperate and reasonably support TomTom (e.g. e-discovery requests or forensic investigations).
10.5	Evidence As part of TomTom's information security incident management process, TomTom may request forensic evidence from the Supplier (e.g. logs). Timelines and formats of evidence must be determined on a case by case basis.

11. Business Continuity Management

Paragraph	
11.1	Business continuity and IT disaster recovery plans The Supplier must have documented and implemented business continuity and IT disaster recovery plans and procedures related to the Deliverables. The plan must be tested at least annually.

11.2	Backups Based on the Deliverables provided, the Supplier must maintain backups of the TomTom's systems and information. Backups must be secured according to standard industry practices.

12. Definitions and abbreviations

Agreement	Any contract signed by TomTom with the Supplier and containing the reference to this ISA.
Assets	Encompass primary and supporting assets as defined in ISO/IEC 27005.
CVE	Common Vulnerabilities and Exposures as defined in: http://cve.mitre.org/index.html.
Deliverables	Any equipment, product and/or service delivered by the Supplier.

Information security	A policy drafted according to or in compliance with ISO/IEC 27001 and ISO/IEC 27005 - security in the scope of information processing and activities (primary assets) relying on technical (including, but not limited to IT, premises, facilities, networks) and non-technical resources (including, but not limited to supporting assets such as staff, partners, organizations, procedures, terms and conditions).
SLA	A service-level agreement (SLA) is a contract between a service provider and its internal or external customers that documents what services the provider will furnish and defines the service standards the provider is obligated to meet.
Vulnerability	A weakness that reduces availability, integrity or confidentiality.
XaaS	Anything delivered to users as a service including SaaS (Software as a Service), PaaS (Platform as a Service), IaaS (Infrastructure as a Service) or similar.