DATA PROCESSING AGREEMENT BETWEEN

**TOMTOM TELEMATICS B.V.**

**AND**

**Full Company Name**

This ”Data Processing Agreement” shall be effective as from \_\_\_\_\_\_\_\_\_\_\_\_\_\_ (“Effective Date”) between:

1. **TomTom Telematics B.V**., a private company, incorporated under the laws of the Netherlands, with its registered seat at De Ruijterkade 154 1011AC Amsterdam, The Netherlands, hereinafter to be referred to as **“Processor**”;

and

1. **Full Company Name** incorporated and registered in **Country of Incorporation** with its registered seat at **Registered Seat**, hereinafter referred to as “**Controller**”;

Controller and the Processor are hereinafter jointly referred to as the “**Parties**” and individually as the “**Party**”.

It is hereby agreed as follows:

1. Definitions

Terms defined in the supply agreement between TomTom and the Controller (“Agreement”) shall have the same meaning when used in this Data Processing Agreement. In addition, the definitions below apply in this Data Processing Agreement:

|  |  |
| --- | --- |
| **GDPR**: | means the EU General Data Protection Regulation; the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995; and |
| **Personal Data:** | means personal data as defined in the GDPR that the Processor processes on behalf of Controller in connection with the Agreement.  Unless otherwise specified, all references to the GDPR shall be understood to be references to the applicable local equivalent which implements said reference into local law. |

1. Subject and Term

The purpose of this Data Processing Agreement is to describe the work to be carried out by the Processor in relation with the Agreement. This Data Processing Agreement forms an integral part of the Agreement hereof. This Data Processing Agreement shall be deemed to take effect from the Effective Date and shall continue in full force and effect until the termination of the Agreement.

1. Scope of the work

The purpose for the collection, processing and use of the Personal Data from Controller is to provide the services as described in the Agreement, which forms an integral part hereof. The processing and use of the Personal Data takes place in a member state of the European Economic area. Any data transfer to a third country requires the prior approval of the Controller.

The processing of the Personal Data by the Processor shall take place within the framework of this Data Processing Agreement and only to the extent that Controller has instructed the Processor to do so in relation with the Agreement. The Processor processes the Personal Data on behalf of Controller. Modifications to the processing of Personal Data under the Agreement are subject to mutual agreement.

The Processor shall not use the Personal Data for any other purpose as described in this Data Processing Agreement.

**Type of data**

The Controller has defined that the following data categories will be collected, processed and used by the Processor under this Data Processing Agreement:

Name, Title, Academic Grade

Professional, commercial or business addresses

Date / Year / Birth Date

Telecommunications data (e. g. connection, location, usage and traffic data)

Telephone Number

Email Address

Contract data (contractual relationship, product and/or contractual interests)

Customer history, contract implementation and payment data

Special data (information about race and ethnic origin, political opinions, religious or philosophical convictions, trade union membership, health or sexuality)

Personal data that is covered by the obligation to maintain professional secrecy

IP addresses

Planning and control data

Precise location data (GPS positions)

Vehicle license plate

**Categories of data subjects**

The Controller has defined the following data subject categories from who the Personal Data as defined above will be collected, processed and used by the Processor under this Data Processing Agreement:

Employees (Internal)

Customers

Contact persons

Employees of external companies

Interested parties

Tenants / landlords, lessees / lessors

Suppliers

1. Technical and organisational measures based on the EU General Data Protection Regulation

The Processor documents the implementation of the technical and organizational measures in accordance with the requirements of the GDPR.

The Processor ensures in particular that it has implemented the appropriate measures to:

1. Prevent unauthorized persons from gaining access to data processing systems with which personal data are processes or used;
2. Prevent data processing systems from being used without authorization;
3. Ensure that persons entitled to use a data processing system have access only to the Personal Data to which they have a right of access, and that personal data cannot be read, copied, modified or removed without authorization during processing or use and after storage;
4. Ensure that personal data cannot be read, copied, modified or removed without authorization during electronic transmission or transport, and that it is impossible to check and establish to which bodies the transfer of personal data by means of data transmission facilities is envisaged;
5. Ensure that it is possible to check and establish whether and by whom personal data has been input into data processing systems, modified or removed;
6. Ensure that, for commissioned processing of personal data, the Personal Data is processed strictly in accordance with the instructions of the Controller (job control).
7. Ensuring the availability of services as described and in accordance with Appendix 1
8. Ensuring the separation of processing as described and in accordance with Appendix 1

Significant changes of the above technical and organisational measures by the Processor shall be agreed by the Parties in writing.

The Processor agrees and warrants that the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the Personal Data to be protected having regard to the state of the art and the cost of their implementation.

The Processor further agrees and warrants that the processing of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law and does not violate the relevant provisions.

1. Processor’s obligations

Under this Data Processing Agreement, the Processor has the obligation to:

1. process the Personal Data only on behalf of the Controller and in compliance with its instructions;
2. ensure that only appropriately trained personnel shall have access to the Personal Data;
3. provide Controller with such cooperation (including access to its facilities) as the Controller may reasonably request;
4. implement such technical and organizational measures to protect the Personal Data as required by the GDPR;
5. notify the Controller immediately of any monitoring activities and measures undertaken by the relevant authority that supervises the applicable data protection legislation;
6. Support Controller regarding Controller’s obligations to provide information about the collection, processing or usage of Personal Data to a data subject;
7. Ensure that the Personal Data is not in any way used, manipulated, distributed, copied or processed for any other purpose than for the fulfilment of the contractual obligations as explicitly agreed upon and arising from this Data Processing Agreement.
8. Sub-processing

The Processor shall not subcontract its obligations under this Data Processing Agreement to a sub-processor without the prior written consent of the Controller unless such sub-processor undertakes, by way of written agreement, substantively the same obligations as imposed on the Processor in this Data Processing Agreement and the Agreement. The Processor shall inform the controller of its intention to engage a sub-processor and the Controller shall have the right to reasonably oppose the appointment of a new sub-processor if the Controller shall have substantive and legitimate reasons for opposing the specific sub-processor and shall notify Processor of such objections in writing as soon as possible after receipt of the Processor’s notice relating to such sub-processor. The addition or removal of a sub-processor should not negatively affect the level of security within the agreement to less than that which existed at the time of signing this Data Processing Agreement.

The Controller shall be granted control and examination rights according to this Data Processing Agreement and the applicable data protection legislation. This also includes the right of the Controller to obtain information from the Processor, upon written request, on the substance of the contract and the implementation of the data protection obligations within the sub-contract relationship, where necessary by inspecting the relevant contract documents. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the Processor shall remain fully liable to the Controller for the performance of the sub- processor's obligations under such agreement.

1. Controller’s rights and obligations

Rights to monitor: Controller is entitled to appoint a third party independent auditor in the possession of the required professional qualifications and bound by a duty of confidentiality, which auditor must be reasonably acceptable to the Processor, to inspect Processor’s compliance with this Data Processing Agreement and the applicable data protection legislation required to determine the truthfulness and completeness of the statements submitted by the Processor under this Data Processing Agreement. Controller’s right to audit shall be subject to giving the Processor at least (4) weeks prior written notice of any such audit.

Processor shall deal promptly and properly with all inquiries from the Controller relating to its processing of the personal data subject to this Data Processing Agreement.

Rectification, deletion and blocking of data: upon instruction by the Controller, the Processor shall correct, rectify or block the Personal Data. Any request from a data subject directly to the Processor, shall be directed to Controller.

1. Information obligations

If the Processor cannot provide compliance or foresees that it cannot comply with its obligations as set out in this Data Processing Agreement, for whatever reasons, it agrees to promptly inform the Controller of its inability to comply, in which case the Controller is entitled to suspend the transfer of data.

Processor will promptly notify the Controller about:

1. any legally binding request for disclosure of the Personal Data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;
2. any accidental, unauthorised access, or other event that constitutes a personal data breach; and
3. any request received directly from the Personal Data subjects without responding to that request, unless it has been otherwise authorised to do so.

The Processor shall indemnify Controller for claims of any third party that arises as a result of Processor’s non-compliance with its obligations under this Agreement and the applicable local laws and legislation of the countries where the Personal Data is processed and regulations regarding data protection and privacy.

1. Principal’s authority to issue instructions

The Processor shall not assign this Data Processing Agreement without the prior written consent of the Controller. Where the Processor assigns this Data Processing Agreement, with the consent of the Controller, it shall do so only by way of a written agreement with the assignee which imposes the same obligations on the assignee as are imposed on the Processor under this Data Processing Agreement.

1. Consequences of termination

The parties agree that on the termination of the provision of the services, the Processor and the sub-processor shall, at the choice of the Controller, return all the personal data transferred including any data storage media supplied to Processor, and the copies thereof to the Controller or shall destroy all the personal data and certify to the Controller that it has done so, unless legislation imposed upon the Processor prevents it from returning or destroying all or part of the personal data transferred. In that case, the Processor warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

1. Confidentiality

Any information of whatever kind (whether technical, commercial, financial, operational or otherwise) and in whatever form (whether oral, written, recorded or otherwise), including Personal Data, (hereafter referred to as “Confidential Information”) which may be disclosed in any form or matter by one Party to the other Party, with respect to, or as a result of this Data Processing Agreement, shall be deemed to be of a confidential nature. Data relating to Controller’s customers database, procedures and knowledge shall be considered as private and confidential information.

1. Other

This Data Processing Agreement is governed by the law that governs the Agreement. Also for the jurisdiction reference is made to the appropriate Section of the Agreement.

AGREED by the parties through their duly authorised representatives on the date both Parties have signed this Data Processing Agreement.

For and on behalf of:

|  |  |
| --- | --- |
| **TomTom Telematics B.V.** | **Full Company Name** |
|  |  |
|  |  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Name: | Name: Full Name |
| Function: | Function: Function |
| Date: | Date: Date dd/mm/yyyy |

**Appendix 1:**

**Technical and Operational Measures**

1. Objective

This appendix is aimed at customers and business partners and sets out the technical and organisational measures for protecting personal data against unauthorised access, corruption and loss in accordance with the EU GDPR and the appendix to Article 9 Clause 1 of the German Federal Data Protection Act (BDSG)) processed by TomTom Development Germany GmbH -Leipzig- in connection with the WEBFLEET services that TomTom Development Germany GmbH -Leipzig- provides to the TomTom Telematics group and its customers.

1. Introduction

The availability of TomTom WEBFLEET services, including the best possible protection for customer data, has top priority and underpins all successful and long-term business relationships.

TomTom Development Germany GmbH -Leipzig- ensures that the latest standards for security and data protection are met and exceeded for WEBFLEET services, including the protection of personal and confidential data. These standards include operating an information security management system (ISMS) in accordance with the ISO 27001:2013 standard.

On-going, comprehensive investments in ground-breaking hardware and software solutions, current technologies and associated processes, policies and audits ensure that the protective measures are complied with and continually improved.

This document provides further details on the technical and organisational measures that have been implemented for data protection purposes.

1. Access control (building / offices / data centre)

TomTom has implemented, but not limited to, the following measures to prevent the unauthorized access to data processing systems where personal data is processed:

|  |  |
| --- | --- |
| Alarm system  Automatic access control system  Photoelectric sensors / Movement detectors  Key Management (Issuance of keys, etc.)  Logging of visitors  Careful selection of security guards  Protection of building shafts  Chip card / Transponder locking system  Manual locking system (Limited usage for key employees to be used in the event of a failure in the access control systems | CCTV at entry points (office and data centres)  Security locks  Visitor management at reception desks  Careful selection of cleaning staff  Visible wearing of access badges mandatory  A separate, specific and documented access control for data centres and server rooms for authorized persons is implemented. Access by authorized persons is documented by name and card or token number. For the data centres, separate access control systems are implemented |

1. Access Control (systems)

TomTom has implemented, but not limited to, the following measures, to prevent the use of data processing systems by unauthorised persons:

|  |  |
| --- | --- |
| Assignment of user rights  Assignment of passwords  Authentication with username / password  Use of Intrusion-Prevention-Systems  Use of Hardware Firewalls  Creation of user profiles  Additional measures: web-application firewalls, regular vulnerability scans, regular penetration testing, patch management, minimum requirements for password complexity and forced password changes, use of virus scanners | Assignment of user profiles to IT systems  Use of VPN Technology  Encryption of mobile storage media  Use of central smartphone administration (for example: remote wiping of smartphone)  Disk encryption on laptops / notebooks  Use of a software firewall (office clients) |

1. Access Control (data)

TomTom has implemented, but not limited to, the following measures, to ensure that authorised users of a data processing system may only access the data for which they are authorised, and to prevent personal data from being read while the data is in use, in motion, or at rest without authorisation:

|  |  |
| --- | --- |
| Creation of an authorization concept  Number of administrators reduced to “absolute necessary”  Logging of application access, especially during the entry, modification and deletion of data  Secure media sanitization before re-use  Use of shredders or services (if possible with privacy seal) | Disk encryption (backup tapes for off-site storage, laptops)  Management of rights by system administrators  Password policy including password length, password change management  Secure storage of data carriers  Logging of secure media destruction  Compliant destruction of data media (DIN 66399) |

1. Transfer control

TomTom has implemented, but not limited to, the following measures, to ensure that personal data cannot be read, copied or modified during electronic transmission or during transportation or storage to disk. Additionally to control and determine to which bodies that the transfer of personal data provided by data communication equipment is allowed:

|  |  |
| --- | --- |
| Creation of dedicated lines or VPN tunnels  Documentation of recipients of data and the time periods for the provision of data including agreed deletion times  During physical transport, careful selection of transport personnel and vehicles (tape off-site storage)  Disk encryption (backup tapes for off-site storage) | Disclosure of data in anonymous or pseudonymous form  Creation of an overview of regular request and delivery operations  During physical transport, secure transport containers / packaging (tape off-site storage)  TLS encryption of all communications (Web-Client, APIs, mobile Apps) |

1. Input control

TomTom has implemented, but not limited to, the following measures, to ensure that it is possible to ensure, subsequently control, and determine if and by whom, personal data has been entered, changed or removed on data processing systems:

|  |  |
| --- | --- |
| Logging of input, modification and deletion of data  Traceability of input, modification and deletion of data by individual user names (not user groups)  Granting of rights for the input, modification or the deletion of data based on an authorization concept | Creation of an overview of which applications are permitted to input, modify or delete which data  Storage of forms, through which data has been acquired during automated processing |

1. Order control

TomTom has implemented, but not limited to, the following measures, to ensure that personal data which is processed by request of the data owner by a data processor, shall only be processed as instructed by the data owner:

|  |  |
| --- | --- |
| Contractor selection via history review (in particular regarding data security)  Written instructions to the contractor (for example, by Data Processing Agreement) (GPDR)  Ensure contractors have appointed Data Protection Officers  Effective control rights over data processors have been agreed | Prior examination of the documentation and the security measures taken by the contractor  Obligation of the contractor’s employees to maintain data confidentiality (GPDR)  Ensure the secure destruction of data after termination of the contract  Continual review of contractors and their activities |

1. Availability control

TomTom has implemented, but not limited to, the following measures, to ensure that personal data is protected against accidental destruction or loss:

|  |  |
| --- | --- |
| Uninterruptible power supplies (UPS)  Devices for monitoring temperature and humidity in server rooms  Fire and smoke detection systems  Alarm when unauthorised entry to server rooms is detected  Testing of data recovery  Secure off-site storage of data backups  In flood areas, server rooms are above the water border | Air conditioning in server rooms  Protection power strips in server rooms  Fire extinguishers in server rooms  Creation of a backup & recovery concept  Preparation of an emergency response plan  Server rooms not located under sanitary installations  Two data centres in Germany in an active/active configuration |

1. Segregated processing

TomTom has implemented, but not limited to, the following measures, to ensure that data which is collected for different purposes can be processed separately:

|  |  |
| --- | --- |
| Creation of an authorisation concept  Provision of records with purpose attributes / data fields  Approved and documented database rights | Logical client separation (in software)  In pseudonymous data : the separation of the mapping file and storage on a separate secured IT system  Separation of production and test systems |

1. Data Protection Officer

The TomTom group has appointed a Data Protection Officer (DPO) in accordance with the EU General Data Protection Regulation (GDPR). This person ensures compliance with the GDPR as well as other relevant global data privacy regulations and other provisions relating to the protection of data.

**Contact Information:**

Mr. Simon Hania

**TomTom Telematics B.V**

<https://www.tomtom.com/en_gb/privacy/>

De Ruijterkade 154, 1011 AC, Amsterdam, The Netherlands

[privacy@telematics.tomtom.com](mailto:privacy@telematics.tomtom.com)

**Appendix 2:**

**Authorised persons to issue / accept instructions**

Persons on the controller's side who are authorised to issue instructions:

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Role | Telephone | Email Address |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Persons on the processor's side who are authorised to accept instructions:

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Role | Telephone | Email Address |
| Michael Oehme | VP IT | +49 341 24495-981 | michael.oehme@tomtom.com |
| Civitas Hall | ISMS Manager | +49 341 24495-981 | civitas.hall@tomtom.com |
| Matthias Graichen | Manager Cust. Support | +49 341 24495-981 | matthias.graichen@tomtom.com |
|  |  |  |  |
|  |  |  |  |

**Appendix 3:**

**Subcontractor directory**

1. Secure data processing based on the ISO 27001:2013 standard, engineering, IT, and data centres in connection with the WEBFLEET services that the TomTom Development Germany GmbH provides to the TomTom Telematics group and its customers: ***TomTom Development Germany GmbH****, Inselstrasse 22, 04103 Leipzig, Germany*

TomTom Development Germany GmbH in Leipzig has appointed an external data protection officer in accordance with the EU GDPR and the (BDSG Article 4f Para. 1). This person ensures compliance with the act and other provisions relating to data protection and handles tasks in accordance with this legislation.

**Contact Information:**

Mr. Christian Volkmer

Projekt 29 GmbH & Co. KG

http://www.projekt29.com

Trothengasse 5, 93047 Regensburg, Germany

Tel. +49 (0) 941-2986930, fax +49 (0) 941-29869316,

privacy@telematics.tomtom.com

Upon request, TomTom Telematics will provide a complete listing of any additional sub-contractors which may be relevant to the processing of data for the purpose of WEBFLEET.