Data Privacy Statement
PTV Navigator G2 App

PTV Logistics GmbH, Sitz der Gesellschaft / Registered Office: Karlsruhe, Geschäftsführung / Management Board: Dr. Steven De Schrijver (Vors./CEO), Dr. An De Wispelaere (CPO), Elmar Weber (CFO), Dr. Marco Di Matteo, Handelsregister (HRB Nr.) / Commercial Register (HRB No.): 745512, USt-ID-Nr. / VAT ID No.: 35007/25076, Registergericht / Court of Registration: Mannheim.

Content

Data Privacy Statement PTV Navigator G2 App 3

1. Responsible Authority 3

2. Registration & activation of the Service 3

3. Use of the Service 4

3.1. Processing performed for all PTV Cloud Services 4
3.2. Product-specific processing 4

4. Data Security 5

5. Order Data Processing 5

6. Processing of personal data when using our Service 5

6.1. Installation 5
6.2. Usage 5
6.3. Cookies 5

7. Data Processing by Third Parties 5

7.1. Third-party providers for all PTV Cloud Services 5
7.2. Product-specific Third-Party Suppliers 6

8. Deletion of Data 8

9. The Client's Right to Information 8

10. Right to log a Complaint with the Competent Supervisory Agency 9

11. Further rights as a data subject 9

Shorttitle	Data Privacy Statement PTV Navigator G2 App
Template history	V2.1.0 dated 2024-06-27

Data Privacy Statement PTV Navigator G2 App

This Data Privacy Statement applies to the use of the PTV Navigator G2 app (the "**Service**") of PTV Logistics GmbH, Stumpfstraße 1, 76131 Karlsruhe, Germany ("**PTV**"), which is made available via the customer access in myptv.com.

General information about our handling of your personal data, as well as data protection information about your registration on myptv.com and the use of the website, as well as about your rights as a data subject, can be received in our general data protection provisions and in the Data Privacy Statement PTV Cloud Service. The Data Privacy Statement PTV Navigator G2 App applies primarily to the use of the PTV Navigator G2 App.

When you use the Service, various personal data is collected. Personal data are data with which you can be personally identified. This data protection declaration explains which data we collect and what we use it for. It also explains how and for what purpose this is done.

1. Responsible Authority

The authority responsible for data processing on the Service is:

PTV Logistics GmbH

Stumpfstraße 1

76131 Karlsruhe, Germany

Email: info@ptvlogistics.com

PTV Logistics GmbH, together with the affiliated companies within the meaning of Section 15 of the German Stock Corporation Act, forms the PTV Logistics Group. PTV Logistics GmbH is also affiliated within the meaning of Sections 15 et seq. Stock Corporation Act (AktG) with PTV Planung Transport Verkehr GmbH, Conundra BV (Belgium) and Conundra B.V. (Netherlands). We may share contact information of customers and interested parties with affiliated companies of PTV Logistics Group and the other affiliated companies mentioned as part of your business relationship (contractual or pre-contractual relationship according to Art. 6 Sect. 1 Sent. 1 lit. b GDPR). The transfer of personal data within the Group for the purpose of contract performance is based on data processing or within the framework of joint responsibility (Art. 28 and Art. 26 GDPR).

We have appointed an external data protection officer for our company, reachable at:

Email: data-protection@ptvlogistics.com

2. Registration & activation of the Service

In order to be able to use the Service, the contractual partner of PTV ("**Customer**") first registered for a myPTV-ID on MyPTV, which serves as an identification number (token ID). With the myPTV-ID the customer then purchased the product PTV Navigator G2 or activated a free trial version. Subsequently, the Customer has provided the user of this Service ("**User**") with a licence key which the User needs to log into this Service and thus activate it.

The General Terms of Service, the Specific Terms PTV Navigator G2, the Product Description PTV Navigator G2 and the Data Privacy Statement PTV Cloud Services shall apply to the use of the Service in their respective applicable version.

The basis for the processing of the authorisation is Art. 6 Sect.1 Sent.1 lit. b GDPR, which permits the processing of data for the fulfilment of a contract, in this case the usage agreement for the Service.

3. Use of the Service

Users have the opportunity to be navigated safely, reliably and on time to their destination through the Service. The Service bypasses unsuitable roads, avoids detours and thus saves time and costs. PTV shall have no influence over the content of the planning or on the processed data. The customer and the user are free to decide which data (for example addresses, station lists or names of, for example, customers or employees) they wish to have processed. Insofar as the Customer or the User processes personal data with the help of the Service, the Customer alone shall be responsible for ensuring that the person concerned in each case has provided consent for its data to be processed or that there is statutory authorisation. The Customer shall always remain the responsible party with regard to such personal data. The Customer shall exempt PTV from all claims of the person concerned and shall compensate PTV for any damage caused to PTV due to transmissions of personal data to PTV in violation of data protection laws, unless the Customer can prove that it is not responsible for this violation.

3.1. Processing performed for all PTV Cloud Services

The processing carried out by us in the same way for all PTV Cloud Services can be found in the Data Privacy Statement PTV Cloud Services.

3.2. Product-specific processing

3.2.1 Probe Data

On the basis of the granted licence from section 4.1 Specific Terms PTV Navigator G2, PTV is entitled to collect any positional or location information data, signal or ping collected on or transmitted or downloaded from a global positioning satellite, device, software program, mobile phone, application or other system or technology, capable of producing or using automatic location detection data regardless of accuracy, that accumulates during the use of the service (“**Probe Data**”)

- to generate real-time information and
- to use such Probe Data for use in connection with its current and future products and services as well as
- to provide such Probe Data to TomTom Global Content B.V., De Ruijterkade 154, 1011 AC, Amsterdam, Netherlands ("**TomTom**") for use in connection with their current and future location technology products and services.

Probe Data is timestamped geolocation data, collected every few seconds, immediately pseudo-anonymised with random temporary ID, subsequently anonymised every 20 minutes, but at the longest within 24 hours of termination of the application or communication severed by deleting association between device/session ID and temporary ID.

Before transmitting Probe Data to TomTom, PTV will truncate start and end points of the Probe Data, subject to the technical and operational conditions set out in the delivery protocol. However, it cannot be ensured through this process that the data is completely anonymised. For the avoidance of doubt, TomTom is not allowed to sell the Probe Data to any third party

The software development kit provided by TomTom and used for the PTV Navigator G2 (see section 7.2.2) additionally divides the distance travelled into segments of random duration, which prevents the journeys from being reassembled. The basis for this processing is Art. 6

Sect.1 Sent.1 lit. b GDPR, which permits the processing of data for the performance of a contract or pre-contractual measures.

4. Data Security

PTV warrants a reasonable level of data security and in particular adheres to the provisions of Art. 32 GDPR.

5. Order Data Processing

PTV concludes a data processing contract with the Customer in accordance with Art. 28 GDPR upon conclusion of the usage contract for a PTV Cloud Service.

6. Processing of personal data when using our Service

6.1. Installation

The installation file of the Service can only be downloaded via myptv.com and sent to the mobile device. During this download via the website, customer data is only processed insofar as this is necessary for the download.

6.2. Usage

When you use the Service, we process the personal data described below to enable you to use the functions comfortably. If you wish to use our Service, we process the following data, which are technically necessary for us to offer you the functions of our Service and to ensure stability and security, so that they must be processed by us. The legal basis is Art. 6 Sect.1 Sent.1 lit. b GDPR:

- IP address
- Date and time of the request
- Time zone difference from Greenwich Mean Time (GMT)
- Access status/HTTP-status code
- Position or location information data, signals or pings
- Installation-ID
- License-Key
- Time-stamped service requests including geolocation data
- Time-stamped service responses
- Transaction log data
- Sum of daily and annual distance travelled in kilometres.

6.3. Cookies

The Service does not use cookies.

7. Data Processing by Third Parties

We also use external service providers for processing your data and handling the contractual relationship. In addition, your data is also processed by us and our affiliated companies as part of other services and applications. In these cases, we ensure the security of your data by concluding commissioned processing contracts with the respective service provider that meet the high legal requirements for data protection compliance.

7.1. Third-party providers for all PTV Cloud Services

The third-party providers we use for all PTV Cloud Services can be found in the Data Privacy Statement PTV Cloud Services.

7.2. Product-specific Third-Party Suppliers

7.2.1 Use of the ML kit from Google for the QR code scan of the licence key

For the Service, we use the ML-Kit Android SDK in the form of an Android library ("**ML-Kit**") from Google Ireland Ltd, Gordon House, Barrow Street, Dublin 4, Ireland. This is a subsidiary of Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA.

The data processed using the ML-Kit is encrypted by the ML-Kit during transmission using HTTPS. The ML-Kit does not transmit this data to third parties.

Further information from Google on the ML-Kit can be found here: https://developers.google.com/ml-kit/android-data-disclosure

The data processed by using the ML-Kit consists of non-personal information and measured values. You can view the data processed when using the ML-Kit in detail here:

Data	**The ML-Kit SDK captures...**
Unit information	Device information (e.g. manufacturer, model, OS version and build) and available ML hardware accelerators. Used for diagnostic and usage analysis.
Information on applications	Package name and app versions. Used for diagnostic and usage analysis.
Device ID or other personal identifiers	For Thin Features: Device ID used for diagnostic and usage analysis. Identifiers per installation that are not used to uniquely identify a user or device. Used for diagnostic and usage analysis. For bundled functions: Identifiers per installation that are not used to uniquely identify a user or device. Used for diagnostic and usage analysis.
Power readings	Performance measures (e.g. latency) Used for diagnostic and usage analysis.
API configuration	API configuration (e.g. image format and resolution). Used for diagnostic and usage analysis.
Event type	Event type (e.g. feature initialisations, model downloads, detection, resource releases). Used for diagnostic and usage analysis.

Error codes	Error code for feature events (e.g. feature initialisations, model downloads, detection, resource releases). Used for diagnostic and usage analysis.

Purpose of data processing: The ML-Kit is used for the sole purpose of enabling users of the Service to scan QR codes. This facilitates the initial entry of the licence key required at the beginning of the app use. Since the key is 64 characters long, we offer the user the option of entering this key by scanning a QR code instead of manually or by copy & paste. The ML-Kit is not used elsewhere in the Service.

Legal basis for data processing: Since only non-personal data is processed here, a legal basis under data protection law is not required. Should such a legal basis nevertheless be required, we have an overriding legitimate interest in this data processing in accordance with Art. 6 Sect.1 Sent.1 lit. f GDPR. The balancing exercise carried out has shown that the interests or fundamental rights and freedoms of the data subjects do not outweigh our interests in. This is because the ML-Kit only processes non-personal information and measured values (see above).

Since the user must actively decide to enable the camera function for scanning the QR code (he or she must activate the camera by clicking on a button) and the user must explicitly allow system-level access to the camera upstream of this step, we assume that the legal basis of consent pursuant to Art. 6 Sect.1 Sent.1 lit. a GDPR is also present.

Duration of storage: The data is only used by us for the above-mentioned purpose and for the duration of the scanning process to compare the licence key and is then deleted. According to Google, it uses the information and measured values to improve its Android SDK. However, this is not personal data (see above).

Possibility of objection and removal: The use of the ML-Kit can be avoided by entering the licence key by copy & paste or manually or by not granting the requested release of the camera for the use of the ML-Kit.

7.2.2 Use of Firebase Crashlytics

We use the Firebase Crashlytics service from Google Ireland Ltd, Gordon House, Barrow Street, Dublin 4, Ireland, to generate crash reports for the app. This is a subsidiary of Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA.

Firebase Crashlytics uses crash stack traces to associate crashes with a project, send email notifications to project members and display them in the Firebase console, and help Firebase customers debug crashes. It uses Crashlytics installation UUIDs to measure the number of users affected by a crash and minidump data to process NDK crashes. The minidump data is stored while the crash session is being processed and then deleted. The Firebase installation ID enables upcoming features that improve crash reporting and crash management services.

The service can be used anonymously, which means that no personal data is involved. However, as we cannot rule out the possibility of the provider receiving, for example, the IP address of the device sending the crash report or other information about this device, this privacy policy is provided as a precautionary measure.

Purpose of data processing: The purpose of data processing is to provide the users of our apps with a reliable and stable service as far as possible. In order to improve the stability and reliability of our apps, we are therefore dependent on anonymised crash reports. In the event of a crash, anonymous information is transmitted to Google's servers in the USA (status of the app at the time of the crash, installation UUID, crash trace, manufacturer and operating system of the mobile phone, last log messages). This information does not contain any personal data.

Legal basis for data processing: Data processing is based on our legitimate interest in accordance with Art. 6 Sect.1 Sent.1 lit. f GDPR . Our legitimate interest lies in the purposes described above. At the same time, it is part of our contractual duties to keep the services offered available for our customers and to be able to react as quickly as possible to crashes and problems with the stability of the services, so that we also base the data processing on the contractual measures in connection with the use of the apps by our customers in accordance with Art. 6 Sect.1 Sent.1 lit. b GDPR .

Duration of storage: Firebase Crashlytics stores crash stack traces, extracted minidump data and associated identifiers (including Crashlytics installation UUIDs and Firebase installation IDs) for 90 days before starting the process of removal from live and backup systems. We ourselves store information in connection with such crash reports as long as the crash exists as an open support ticket with us.

Possibility of objection and removal: In the Android apps, it is possible to deactivate the sending of crash reports across all apps. This is done in the Android settings. To do this, open the Settings app, select the "Google" item and then the "Usage & diagnostics" menu item in the three-dot menu at the top right. Here you can deactivate the sending of the corresponding data. Further information can be found in the help for your Google account.

Further information on data protection can be found in the Firebase Crashlytics privacy policy at https://firebase.google.com/support/privacy and at https://firebase.google.com/#data-collection-policies.

7.2.3 Using the Navigation SDK for Android from TomTom

The operation of the Service and thus the processing of the personal data that you would like to have processed via PTV Navigator G2 or this Service is carried out with the help of the Navigation SDK for Android ("**Navigation SDK**") provided by TomTom.

The basis for the processing of Probe Data is Art. 6 Sect.1 Sent.1 lit. b GDPR, which permits the processing of data for the performance of a contract or pre-contractual measures.

The basis for the processing of your personal data that is not Probe Data is based on our legitimate interest according to Art. 6 Sect.1 Sent.1 lit. f GDPR.

An agreement on commissioned processing exists between PTV and TomTom.

For more privacy-related information about the TomTom SDK for Android, please visit https://www.tomtom.com/en_gb/privacy/.

8. Deletion of Data

PTV shall delete all user data within 8 weeks after terminating the contractual relationship. If PTV is obliged by legal data storage requirements to retain the user's data (e.g. invoice and contract data), PTV will block this data for further processing.

9. The Client’s Right to Information

Pursuant to Art.15 GDPR, data subjects may at any time request information on the per-sonal data stored by PTV on them or their pseudonym. Requests for information can be addressed to:

PTV Logistics GmbH

Stumpfstraße 1

76131 Karlsruhe, Germany

Email: data-protection@ptvlogistics.com

10. Right to log a Complaint with the Competent Supervisory Agency

In the event of violations of the GDPR, data subjects are entitled to log a complaint with a supervisory agency, in particular in the member state where they usually maintain their domicile, place of work or at the place where the alleged violation occurred. The right to log a complaint is in effect regardless of any other administrative or court proceedings available as legal recourses.

11. Further rights as a data subject

A complete list of all data subject rights can be found in the Data Privacy Statement PTV GmbH.