Privacy Notification Guidelines

Your users should be suitably informed in a Privacy Notification about how personal data is used. Personal data can be data the user has provided or data that is automatically collected or generated. This includes data attached to unique serial numbers, such as device id's, MAC addresses, IP-addresses and cookies.

The description of the data and the collection and usage of the data, should be presented in a way that is understandable to the user. The information should be clear and specific, and not written in a legal style. To avoid confusing the user with large amounts of small print, the information should be structured, with sub-sections added where it will help in understanding the text.

This Privacy Notification should be available and accessible at all times. The Privacy Notification should be presented before any data collection has started, either by presenting the Notification directly on the screen, or by providing a button or a link to the Notification.

Note: The guidelines below are meant to help software developers adhere to the notification requirements imposed by EU privacy/data protection laws and to align with the way in which TomTom adheres to those laws. It is not a comprehensive legal advice nor should it be interpreted as such: the entity delivering the app or service remains responsible and accountable for the associated privacy issues.

The Privacy Notification should contain the following descriptions:

- **Context:** Add a short explanation of the app, service or feature, including what it does, why it exists, what benefits it delivers and to whom.
- **What:** Describe the data that is collected from the user. To improve clarity, the description can consist of the categories of data and include examples, but does not necessarily have to list all individual data elements.
- **Why:** Briefly explain the various purposes the data will be used for, in a way that the user can understand and so is able to determine each individual application of the data. If automated decisions are made based on the data (for example by applying profiles), the logic being used should also be described.
- **When:** Briefly explain when the data will be destroyed or anonimised. The retention period of the data should be clearly related to the purposes it is used for, and that period should not be excessive.
- **Who:** State clearly which entities have access to the data, in particular those entities which are able to independently decide why and how the data is used, which ones have a responsibility towards the user, and which ones can be held accountable. Examples of accountable entities could be providers of SDKs and services for analytics, social media, advertising, crash reports, etc. For this reason contact details should be provided so the user can request and obtain further information as well as to view and correct collected personal data. The user also have to be able to prevent further use of the personal data (to the extent that it is possible) and be informed about how to achieve that.
- **Where:** The location where the data is used is relevant as it is a factor in determining which specific laws are applicable and which governments and/or authorities can get involved. However the main reason is for the user to be made aware when a transfer of personal data out of the European Economic Area (EEA) is performed and to what extent additional contractual arrangements are in place that effectively impose obligations from EU privacy laws on all receiving entities.
- **Additional and miscellaneous info:** Add any additional information that is useful to help the user understand what is happening to personal data and to provide reassurance, based on the functions specifics of the app or service. For example, explain how the personal data is protected by security measures against unauthorized access, state to what extent law enforcement entities could obtain access, and add helpful and relevant references to external material or sites.

Background information:

Joint European Data Protection Authorities "Opinion 02/2013 on smart devices", page 22 and subsequent:
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf

Joint European Data Protection Authorities "Opinion "Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting"
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp224_en.pdf

The European Data Protection Directive (95/46/EC):
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML