Privacy Notice

In this Privacy Notice, we would like to explain how we process your personal data when you use the platform and its functions.

Introduction

What is personal data?

The General Data Protection Regulation (GDPR) defines in Article 4 Paragraph 1 what is meant by personal data:

"any information relating to an identified or identifiable natural person (hereinafter referred to as the "data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; […]."

1. Name and contact details of the controller and data protection officer

This Privacy Notice applies to data processing by the controller:

Transporeon GmbH
Heidenheimer Straße 55/1
89075 Ulm
Germany
+49 731169060
info@transporeon.com

1.1. Data protection officer of the controller

Data protection queries can be sent to the data protection officer at Transporeon via e-mail to **transporeon_dataprotection@trimble.com** or you can send your request by post to the following address:

Transporeon GmbH
Data Protection Officer
Heidenheimer Straße 55/1
89075 Ulm
Germany

2. Collection and storage of personal data and the nature and purpose of its use

2.1. When visiting the platform

When you visit our platform, the browser used on your device automatically sends information to the server of our platform. This information is temporarily stored in what is referred to as a log file. The following information will be collected without your intervention and stored until automated deletion at the latest 1 calendar year after the last sign-in:

- IP address of the requesting computer
- userID (including corresponding e-mail address upon incorrect sign-in)
- Date and time of access
- Name of the accessed URL
- Website from which access is made (referrer URL)
- Browser used and, if applicable, the operating system of your computer as well as the name of your internet service provider

The data given is processed by us for the following purposes:

- Ensuring smooth connection to the platform
- Ensuring convenient use of our platform (e.g. by optimising the presentation)
- Prevention of fraud and misuse of the platform (e.g. through account sharing)
- Evaluation of system security and stability

The legal basis for data processing here is Art. 6 Para. 1 clause 1 lit. f GDPR. Our legitimate interest arises from the data collection purposes listed above.

In addition, we use cookies relating to visits to our platform. Further details can be found in section **5 (Cookies)** of this Privacy Notice.

2.2. When using the platform

The platform is a service that enables shippers, carriers, suppliers and goods recipients to optimise their logistics processes, especially through the exchange of transport data. The users of the platform are persons who work for such companies.

2.2.1 Which data do we process? – Platform user

The majority of the data on the platform is not personal data, but transport-related data. For example, this data could be routes, offers, or transport documentation.

We save transactions you carry out on the platform, for example, the placing or accepting of transport offers, changing of a transport status or booking of a time slot for the delivery of goods.

Furthermore, your following personal data will be processed:

- First name
- Last name
- Business contact details
- Non-persistent installation ID*

* Please note, that the latter one is only processed if you are using our Transporeon Planner app to browse the platform from your mobile device. This ID allows us to send you push notifications to your mobile device.

2.2.2 Which data do we process on behalf of business customers? – Drivers (e.g. driver of the transport)

This privacy notice is specifically aimed at platform users. If you read this privacy policy as a driver of a transport and related to the usage of Road Visibility and/or Carbon Visibility products, we process your data on behalf of business customers as data processor (except for the usage of Transporeon Trucker). In our role as data processor and customer as data controller, it is an obligation of your employer to ensure a legal basis and inform you about the details of the data processing. We have summarised the default processing in the following information statement in order to assist our business customers with their information obligations: **https://legal.transporeon.com/DP/RTV/en_Driver_Privacy_Policy.pdf**. Please note, that your employer might deviate from this.

2.2.3 Why do we process your personal data?

We process transactions that you perform on the platform to provide transparency and traceability of the transport process to your company and your business partners (processing and placement of transport assignments).

The processing of your first name, last name, and business contact details takes place when using the platform (including access to the platform, communication with users, remote support and onboarding, information on updates and troubleshooting).

The processing of your non-persistent installation ID takes place when using our Transporeon Planner app (see above). What notifications you receive can be setup directly on your mobile device.

The legal basis for data processing is Art. 6 Para. 1 clause 1 lit. f GDPR and results from our legitimate interest in operating the platform.

2.2.4 For what period of time will your personal data be saved?

Your personal data will be deleted from the interactive applications of the platform at the latest after 90 calendar days. The data will be deleted from the active database of the platform at the latest after 3 calendar years after the transport process, whereby the 3-year period begins in the year after the transport process.

The interactive platform describes the respective platform in live operation. After the data are deleted there, they can only be seen by platform users through the Reporting Tool. The Reporting Tool can only be used by activated platform users, and they can only see that data for which they are otherwise authorised.

2.3. When registering for our newsletter

If you have expressly consented in accordance with Art. 6 Para. 1 clause 1 lit. a GDPR in the user menu under “Settings” or already in the registration centre, we will use your e-mail address to regularly send you our newsletter. This newsletter relates to the area of transport logistics process optimisation for our affiliated companies named under section **3 (Disclosure of data)**, and includes, for example, industry information, product updates, results of completed analyses, and case studies from reference customers.

2.3.1 Revocation of consent/cancellation

You can revoke your consent to the sending of our newsletter at any time by unsubscribing. You can unsubscribe by clicking on the link provided in every newsletter e-mail, directly via “Settings” in the user menu, or by sending an e-mail to **unsubscribe@transporeon.com**.

2.4. When using the registration centre

The registration centre is a website to register the platform and complete the contract related to it. On this website, you have the option to update your contract as well as make additional contracts. The registration centre is used exclusively by carriers and suppliers.

We process all data requested there (such as first name, last name, business contact data, e-mail address, telephone number) for the purpose of contract fulfilment in accordance with Art. 6 Para. 1 clause 1 lit. b GDPR; to permit you to use the platform and support you while using it or – if you are not the contractual partner – to safeguard our legitimate interests in the operation of the registration centre in accordance with Art. 6 Para. 1 clause 1 lit. f GDPR.

2.5. When using the Administration Portal

On the Administration Portal (My Transporeon), shippers, carriers, suppliers and goods recipients are given the opportunity to edit their data.

The main users of your company can view and access your personal data in order to manage the user accounts of your company. They can also see which transactions you and the main users have carried out on the platform.

In addition, they can edit your business phone and e-mail contact details as well as see and save invoices.

We process all data requested there (such as first name, last name, business contact data, e-mail address, telephone number) for the purpose of contract fulfilment in accordance with Art. 6 Para. 1 clause 1 lit. b GDPR; to permit you to use the platform and support you while using it or – if you are not the contractual partner – to safeguard our legitimate interests in the operation of the Administration Portal in accordance with Art. 6 Para. 1 clause 1 lit. f GDPR.

2.6. When using Freight Marketplace

Freight Marketplace enables shippers, carriers, suppliers and goods recipients to offer and request freight services and other related logistics services. The goal is to help them find the right counterpart, increase price transparency and facilitate transactional efficiency.

Furthermore, a user may, at their own discretion, create a general profile page of their respective company and provide further business related personal and non-personal information in order to facilitate business cooperation in Freight Marketplace. This information is visible to all other users in Freight Marketplace.

We process all data requested there (such as first name, last name, business contact data, e-mail address, telephone number) for the purpose of contract fulfilment in accordance with Art. 6 Para. 1 clause 1 lit. b GDPR; to permit you to use the platform and support you while using it or – if you are not the contractual partner – to safeguard our legitimate interests in the operation of Freight Marketplace in accordance with Art. 6 Para. 1 clause 1 lit. f GDPR.

3. Disclosure of data

If you carry out transactions with a different user on the platform, this user can see your first name, last name and business contact details. These business contact details are limited to those details necessary for the logistics process between you (or your company) and the company of this user. In addition, your personal data are also displayed to those companies with which you or your company are in a business relationship. They are also displayed to users with whom you are in contact through the platform's messaging function.

We provide your personal data to our affiliate companies, which are named at the following address:
https://legal.transporeon.com/transporeon_entities.pdf

In addition, depending on the use of our services, we currently provide your personal data to the following service providers, which are named at the following address: **https://legal.transporeon.com/transporeon_service_providers.pdf**

If you decide to make use of any services offered by the external partners, available on Freight Marketplace, your personal data will be also shared with the respective external partners, which are named at the following address:
https://legal.transporeon.com/transporeon_external_partners.pdf.

We process your personal data on servers based in Germany, unless otherwise stated. If you work with users from countries outside the European Union or the European Economic Area, they can view your above-mentioned personal data on our platform.

The European affiliated companies of Transporeon and the affiliated companies outside of the European Union or the European Economic Area have implemented the EU standard contractual clauses in order to ensure an adequate level of data protection and to ensure compliance with the legal requirements of Art. 44 ff. GDPR.

The legal basis for data transmission is Art. 6 Para. 1 clause 1 lit. f GDPR. Our legitimate interest results from the possibility to support your use of our service worldwide and in a multitude of languages.

4. Trimble Arc Agent

This section applies exclusively to users who make use of Trimble Arc Agent (hereinafter “Arc Agent”). If you do not use Arc Agent, the processing described in this section does not apply to you.

Arc Agent is a specialised AI assistant designed to help you navigate logistics and transport tasks with greater speed and reliability. It combines information retrieval from Transporeon and Trimble resources with generative language models to deliver answers and outputs tailored to your operational needs. Arc Agent can also orchestrate a governed set of skills, which are specific capabilities allowing it to interact securely with external tools, databases, and APIs, each of which has undergone internal technical and legal review. Arc Agent acts strictly as an informational and task-oriented tool on the basis of your instructions and does not make autonomous operational decisions on your behalf.

When you use certain skills, Arc Agent may process personal data to fulfil your request. The personal data processed in this context includes your user identity and account information, your e-mail address, chat messages and prompts exchanged through the interface, including the text of your voice prompts. We have implemented automated techniques to minimise the exposure of personal data within your prompts. More broadly, in connection with the processing of your personal data through Arc Agent, we have adopted the following data protection commitments: we do not use your personal data to train the underlying language models; your organisation’s data is never used to personalise the AI for other customers; Arc Agent does not make solely automated decisions with significant legal effects; we do not sell your personal data to third parties; and personal data is retained for between 30 days and 3 years from your last interaction, after which it is automatically deleted or anonymised.

Where Arc Agent accesses personal data stored within the platform or other Trimble products through its skills, this personal data held in those other Trimble products is stored in pseudonymised form, with personally identifiable information masked at rest (meaning while it is securely saved in storage). In all such cases, the remainder of this Privacy Notice applies in full. We recommend avoiding entering unnecessary personal or sensitive information into Arc Agent.

The legal basis for this processing is Art. 6 Para. 1 clause 1 lit. f GDPR, based on our legitimate interest in providing an efficient and reliable AI-assisted experience within the transportation and logistics sector, including offering you a convenient and accessible way to interact with Arc Agent by voice inputs.

Arc Agent for Negotiations, a skill available within Arc Agent, generates negotiation plans, playbooks, role-play simulations, and draft negotiation messages. Where you choose to use its optional voice interaction feature to practise a negotiation out loud, your spoken voice is processed by our voice technology provider to generate the interaction. This specific processing takes place only with your consent under Art. 6 Para. 1 clause 1 lit. a GDPR, which you can give or withdraw at any time in the skill's settings; doing so does not affect the other, non-voice functions of the skill.

5. Cookies

5.1. Session and Setting Cookies

We use session cookies on our platform. These are small files that your browser automatically creates and that are stored on your device (laptop, tablet, smartphone, etc.) when you visit our platform. Cookies do not harm your device, do not contain viruses, trojans or other malicious software. The cookie stores information resulting in connection with the specific terminal used. However, this does not mean that we are immediately aware of your identity. The use of cookies serves to make using our online services more pleasant for you. And so we set so-called cookies to authenticate you. In addition, we also use temporary cookies that are stored on your device for a specified period of time. If you visit our platform again to use our services, we automatically recognise that you were already on our site and note what language you chose, so you will not have to enter it again. These cookies are automatically deleted after a defined time. The data processed by cookies is required for the purposes of safeguarding our legitimate interests as well as those of third parties pursuant to Art. 6 Para. 1 clause 1 lit. f GDPR.

5.2. Acceleration of the platform through Cloudflare

We use delivery, security, and analysis services from Cloudflare Inc., 101 Townsend St., San Francisco, CA 94107, USA (hereinafter “Cloudflare”). These services use cookies, text files, beacons, and browser interfaces that generate log files that permit Cloudflare (i) to deliver the platform quickly, reliably, and securely, (ii) perform analyses on the performance of the platform and the related user experience, (iii) conduct security analyses (iv) and prevent unallowed access to the platform, (v) and create reports about (i) to (iv) for its customers. The log files that are generated can contain personal data in the form of IP address, activities on the platform and evaluation of your use of the platform. Cloudflare can pass these data on to third parties if Cloudflare is legally required to do this or if the third parties process these data on assignment from Cloudflare. Cloudflare can transfer the data to its server as well as store and process it there. The Cloudflare servers are located mainly in the USA. Cloudflare makes sure that the transfer of personal data of EU citizens outside the European Economic Area meets the requirements of the relevant data privacy laws. For this purpose, Cloudflare has implemented legally recognised transfer mechanisms: the EU standard contractual clauses. Additionally, an adequacy decision from the European Commission is in place for the USA and Cloudflare Inc. complies with the EU-U.S. Data Privacy Framework (DPF). To learn more about the DPF program and to view the certification, please visit **https://www.dataprivacyframework.gov/**. Cloudflare does not use the data to identify natural persons or for profiling of natural persons.

The legal basis for data processing is Art. 6 Para. 1 clause 1 lit. f GDPR and results from our legitimate interest in a platform that can be reached quickly worldwide along with the related security analyses.

More information on the terms of use for processing personal data by Cloudflare and on the Cloudflare data privacy guidelines can be found at **https://www.cloudflare.com/privacypolicy/**.

5.3. Use of Google reCAPTCHA

We use "Google reCAPTCHA" (hereinafter "reCAPTCHA") in our registration centre as well as on our platform. The supplier is Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland (hereinafter "Google"). reCAPTCHA checks whether the data entry in our registration centre (e.g. In the registration form) and on our platform (e.g. on the sign-in page) was made by a person or by an automated program (e.g. bot). To do this, reCAPTCHA analyses the behaviour of your visit using various characteristics. This analysis begins automatically as soon as you visit our registration centre or our platform. In the analysis, reCAPTCHA analyses various types of information (e.g. IP address, your length of stay on the platform, or the mouse movements you made). The data recorded in the analysis is passed on to Google. The data is processed by Google inside the European Union and possibly also in the USA. For this purpose, Google has implemented legally recognised transfer mechanisms: the EU standard contractual clauses. Additionally, an adequacy decision from the European Commission is in place for the USA and the mother company, Google LLC (located in the USA) complies with the EU-U.S. Data Privacy Framework (DPF). To learn more about the DPF program and to view the certification, please visit **https://www.dataprivacyframework.gov/**.

The legal basis for processing the data is Art. 6 Para. 1 clause 1 lit. f GDPR and results from our legitimate interest to protect our registration centre and our platform from the misuse of automated spying, automatic registration, and spam.

The reCAPTCHA analyses run completely in the background. You as user are not informed that an analysis is taking place. Further information on Google reCAPTCHA as well as Google's data privacy statement can be found at: **https://policies.google.com/terms?hl=en** and **https://policies.google.com/privacy?hl=en**.

5.4. Pseudonymised statistics in Network Insights

Within our service Network Insights we use cookies from QuickSight, AWS' business intelligence tool (Amazon Web Services Inc., 410 Terry Avenue North, Seattle, WA 98109-5210, USA; hereinafter "QuickSight") to measure and analyse metrics and statistics related to user behaviour within this service. The analysis exclusively focuses on aggregated data, such as, for instance, the percentage of user engagement or a number of active users in total, without identifying or reporting on specific individuals. For the purposes of such an analysis the user's name and e-mail address are not stored but instead replaced with a pseudonymised ID, i.e. random alphanumeric strings. Neither direct identifiers, nor the pseudonymised IDs are displayed in any aggregated statistics and are exclusively used to produce an aggregated overview. For these purposes we use functions of QuickSight, with servers in the European Union. Respectively all data stays within our AWS environment and is not shared with any further third parties. The data is processed by Amazon inside the European Union and possibly also in the USA. For this purpose, Amazon has implemented legally recognised transfer mechanisms: the EU standard contractual clauses. Additionally, an adequacy decision from the European Commission is in place for the USA and Amazon Web Services Inc. complies with the EU-U.S. Data Privacy Framework (DPF). To learn more about the DPF program and to view the certification, please visit **https://www.dataprivacyframework.gov/**.

Analytical data that can be traced back to any pseudonymised ID is retained for 13 months, after which it is permanently deleted. The legal basis for processing the data is Art. 6 Para. 1 clause 1 lit. f GDPR and results from our legitimate interest to improve and optimise Network Insights and user experience by understanding user engagement and conversion rates.

5.5. Datadog

We use the web analytics tool "Real User Monitoring" provided by Datadog, Inc., 620 8th Avenue, Floor 45, New York, NY 10018, USA (hereinafter "Datadog") to receive anonymous usage analysis of the platform, such as overall use and traffic, as well as for error detection and corrections. Datadog collects performance and error data in users' browsers without collecting user names or e-mails; the only personal data collected is a pseudo-anonymised user ID. This enables us to automatically identify errors, investigate them depending on the user's settings, and fix the errors in a timely manner. In some cases, Datadog logs may include session recordings reconstructed from user mouse movements to help us investigate potential issues and ensure our users have the best experience. These sessions do not contain any personal data of users, and all personal data in the user interface is masked for this purpose. All data collected and transferred to Datadog, such as user ID, organisation ID, browser meta data, and anonymous session recordings, is stored on servers in the EU, since we have opted for the EU server instance. We delete anonymous analytics data, any log data linked with pseudo-anonymised IDs, as well as any session recordings every two months. Datadog is certified under the EU-U.S. Data Privacy Framework (DPF). To learn more about the DPF program and to view the certification, please visit **https://www.dataprivacyframework.gov/**. For more information about Datadog's privacy policy, please refer to: **https://www.datadoghq.com/legal/privacy/**. The legal basis for data processing here is Art. 6 Para. 1 clause 1 lit. f GDPR. Our legitimate interest arises from the data collection purposes listed above.

6. Analysis tools/Tracking

6.1. Hotjar

We use functions of the web analysis service Hotjar Inc., Level 2, St. Julian's Business Centre, 3, Elia Zammit Street, St. Julian's STJ 1000, Malta (hereinafter "Hotjar"). We use Hotjar because it helps us better understand your experience (e.g. how much time you spend on which pages, which links you choose to click, what you do and don't like, etc.) and this enables us to build and maintain our platform with user feedback. Hotjar uses cookies and other technologies to collect data on your behaviour and your devices. This includes a device's IP address (we use Hotjar's anonymisation function). This shortens your IP address and ensures that the analysis data is not personally identifiable. We do not

merge the data with other personal data, device screen size, device type (unique device identifiers), browser information, geographic location (country only), and the preferred language used to display our platform. Hotjar stores this information on our behalf in a pseudonymised user profile. Hotjar is contractually forbidden to sell any of the data collected on our behalf. For further details, please see the 'about Hotjar' section of Hotjar's support site: **https://help.hotjar.com/hc/en-us/articles/360045420794**. We delete the analytics data about your visit after 12 months.

The legal basis for the web analysis is your consent according to Art. 6 Para. 1 clause 1 lit. a GDPR. You can revoke your consent in "My Transporeon" on our platform at any time. Your data are then no longer used for web analysis. Further information on the opt-out can be found at: **https://www.hotjar.com/legal/compliance/opt-out/**.

6.2. Mixpanel

We use functions of the web analysis service Mixpanel Inc., One Front Street, 28th floor, San Francisco, CA 94111, USA (hereinafter "Mixpanel"). We use Mixpanel because it allows us to measure product KPIs like churn, retention, usage frequency, usage duration, etc. and it helps us to better understand how you interact with our products (e.g. which features are most/least used, where do you spend the most time, etc.) which will in return help us to decide where to improve our products. Mixpanel uses cookies and other technologies to collect data on your behaviour and your devices. We setup Mixpanel that no personal information is being stored and a distinct ID is used for detecting if it is a new user or a recurring visitor. This distinct ID is created by us and then sent to Mixpanel. Mixpanel cannot merge the tracking data with other personal data on their end. However, we are able to do this since the distinct ID equals your user ID within our services. It contains personal data like your name or business contact details that you have stated in your user profile. For further details, please see the Mixpanel Privacy Statement: **https://mixpanel.com/privacy/**. We delete the analytics data about your visit after 26 months.

With Mixpanel we have implemented the EU standard contractual clauses in order to ensure an adequate level of data protection and to ensure compliance with the legal requirements of Art. 44 ff. GDPR. Additionally, an adequacy decision from the European Commission is in place for the USA and Mixpanel complies with the EU-U.S. Data Privacy Framework (DPF). To learn more about the DPF program and to view the certification, please visit https://www.dataprivacyframework.gov/. The legal basis for the web analysis is your consent according to Art. 6 Para. 1 clause 1 lit. a GDPR. You can revoke your consent in "My Transporeon" on our platform at any time. Your data are then no longer used for web analysis. Further information on the opt-out can be found at: **https://mixpanel.com/optout/**.

The above also applies to users of the Trimble Arc Negotiations skill. The following differences apply in that context. Unlike the general platform tracking described above, the distinct ID used for Arc Negotiations is a randomly generated, device-based identifier. No Transporeon or Trimble user account identifier is used as the distinct ID, and neither we nor Mixpanel can directly link the distinct ID to your individual user account. Mixpanel cannot merge the tracking data with other personal data on their end. We may, however, technically be able to correlate analytics events with your user account by reference to other identifiers transmitted as part of those events, such as project or session identifiers associated with your account in our systems. This form of correlation is more indirect than under the general platform tracking described above, where the distinct ID directly corresponds to your user account. The data that could thereby be linked to you may include personal data such as your name or business contact details that you have stated in your user profile. For further details, please see the Mixpanel Privacy Statement: **https://mixpanel.com/privacy/**. We delete the analytics data after 26 months. The international data transfer safeguards described above, including the EU standard contractual clauses and the EU-U.S. Data Privacy Framework, apply equally to this processing. The legal basis for the web analysis is your consent according to Art. 6 Para. 1 clause 1 lit. a GDPR. You can revoke your consent in the Settings of this skill at any time. Your data are then no longer used for web analysis. Further information on the opt-out can be found at: **https://mixpanel.com/optout/**.

6.3. Gainsight

Gainsight, provided by Gainsight, Inc., 350 Bay Street Suite 100m San Francisco, CA 94133, USA (hereinafter "Gainsight") is an analytics, feedback, and product management tool. We use Gainsight to capture user behaviour and interactions with the platform, provide automated context-aware help, and optionally capture in-product feedback from a user about the application. We use the captured analytics to generate reports, track feature usage, and ultimately improve the user experience and product. The data collected will be linked to your account on the platform, i.e., your name and your e-mail address as provided in the course of your account registration. We delete the analytics data about your visit after 26 months.

The legal basis for this processing is your consent according to Art. 6 Para. 1 clause 1 lit. a GDPR. You can revoke your consent in "My Transporeon" on our platform at any time. Your data is then no longer used for the analysis by Gainsight tool. Gainsight is certified under the EU-U.S. Data Privacy Framework (DPF). To learn more about the DPF program and to view the certification, please visit **https://www.dataprivacyframework.gov/**. For more information about Gainsight's privacy policy, please refer to: **https://www.gainsight.com/policy/privacy/**.

7. Rights of the data subject

Given below is information on your rights in connection with your personal data:

- According to Art. 15 GDPR, you may request information about your personal data processed by us. In particular, you can request information on the processing purposes, the category of personal data, the categories of recipients to whom your data has been disclosed, the planned retention period, the rights to rectification, deletion, limitation of processing, or objection, the existence of a right to complain, the source of the data, if not collected from us, and the existence of automated decision-making including profiling and, where appropriate, meaningful information about the details;

- According to Art. 16 GDPR, you may immediately demand the correction of incorrect or completion of incomplete personal data stored with us;
- According to Art. 17 GDPR, you may also request the deletion of your personal data stored by us, unless processing such data is required for the exercise of the right to freedom of expression and information, for the fulfilment of a legal obligation, for reasons of public interest, or for assertion, exercise or defence of legal claims;
- According to Art. 18 GDPR, you may request the limitation of processing of your personal data if the accuracy of your data is disputed, the processing is unlawful, but if you decline the deletion of such data and we no longer require the data, however you require the data for the assertion, exercise, or defence of legal claims, or if you have objected to the data processing in accordance with Art. 21 GDPR (see section **8 (Right to object)**);
- According to Art. 20 GDPR, you may receive your personal data provided to us in a structured, standard and machine-readable format or require it to be forwarded to another controller;
- According to Art. 7 Para. 3 GDPR, you may revoke your consent previously given to us at any time. As a result, we are not permitted to continue the data processing based on this consent for the future and
- According to Art. 77 GDPR, you may complain to a supervisory authority. You are normally permitted to contact the supervisory authority of your usual place of residence or workplace or our registered office (see **https://www.bfdi.bund.de/DE/Service/Anschriften/anschriften_table.html** (only available in German)).

8. Right to object

If your personal data is processed based on legitimate interests in accordance with Art. 6 Para. 1 clause 1 lit. f GDPR, you have the right to file an objection against the processing of your personal data in accordance with Art. 21 GDPR provided that there are reasons for this arising from your particular situation, or the objection relates to direct advertising. In the latter case, you have a general right of objection, which is implemented by us with no requirement to give a specific reason. If you would like to exercise your right of revocation or objection, please send an e-mail to **transporeon_dataprotection@trimble.com**.

9. Singapore “Personal Data Protection Act 2012”

This data privacy statement is based on the GDPR. This data privacy statement may continue to apply for all personal data collected, used, transferred or otherwise processed in Singapore in the framework of the “Personal Data Protection Act 2012 ("PDPA")”. In this case, the following supplement shall apply: **https://legal.transporeon.com/DP/SGP/Singapore_Privacy_Policy.pdf**.

10. Other questions

If you have further questions about your personal data that were not answered here, please contact us at **transporeon_dataprotection@trimble.com**.