

TRATON Charging Solutions AB – Privacy Notice

Last updated: January 2026

TRATON Charging Solutions AB ("TCS", "we", "us" in any form) care about the protection of your personal data. This privacy notice ("Privacy Notice") contains information about how TCS processes your personal data in connection with your use, e.g. through your employer, of the TCS eMSP Service as either a driver or an administrator. This Privacy Notice includes information about what personal data we process about you, for which purposes the personal data is processed and with whom we may share your personal data.

Any fleet manager, or whoever implements the use of the TCS eMSP Service within its operations, has an obligation to provide this privacy notice to relevant data subjects (inter alia employees and drivers). If you have any questions or concerns regarding our processing of your personal data, please contact us via the contact information below.

"**Applicable Data Protection Law**" means legislation applicable from time to time, such as laws and regulations, including provisions issued by the relevant supervisory authorities, regarding the protection of the fundamental rights and freedoms of natural persons and, in particular, the right to protection of their personal data applicable to current processing, including: (i) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) ("**GDPR**"); (ii) the GDPR, as transposed into United Kingdom national law by operation of section 3 of European Union (Withdrawal) Act 2018 and subsequently amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 ("**UK GDPR**"); and (iii) the Data Protection Act 2018, as well as legislation, laws and regulations supplementing the GDPR and the UK GDPR.

For Bulgaria, "Applicable Data Protection Law" also includes the Personal Data Protection Act, as amended, and the secondary legislation on its application.

For Croatia, "Applicable Data Protection Law" also includes the Act on the Implementation of the General Data Processing Regulation (Official gazette of the Republic of Croatia No. 42/2018).

For Cyprus, "Applicable Data Protection Law" also includes Law 125 (I)/2018 of 31 July 2018 implementing certain provisions of and supplementing the

GDPR in Cyprus and Law 112(I)/2004 of 30 April 2004 on Regulation of Electronic Communications and Postal Services.

For Czech Republic, “Applicable Data Protection Law” also includes the Czech Act No. 110/2019 Coll., on processing of personal data, as amended, implementing the GDPR in Czech Republic.

For Estonia, “Applicable Data Protection Law” also includes the Estonian Personal Data Protection Act of 12 December 2018 (as amended from time to time) and other Estonian national law regulating the processing of personal data.

For France, “Applicable Data Protection Law” also includes Act No. 78-17 of January 6, 1978 on computing, files and civil liberties as last amended (“**FDPA**”) and Decree No. 2019-536 of May 29, 2019 adopted for the application of the FDPA.

For Hungary, “Applicable Data Protection Law” also includes Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (“**Infotv**”).

For Iceland, “Applicable Data Protection Law” also includes the Icelandic Act on Data Protection and the Processing of Personal Data No. 90/2018, implementing the GDPR.

For Italy, “Applicable Data Protection Law” also includes Legislative Decree n. 196/2003 (“**Italian Privacy Code**”).

For Latvia, “Applicable Data Protection Law” also includes Personal Data Processing Law of 5 July 2018 and Law on Information Society Services of 1 December 2004.

For Lithuania, “Applicable Data Protection Law” also includes the Law of Republic of Lithuania on Legal Protection of Personal Data of 11 June 1996 (as amended from time to time, available at https://vdai.lrv.lt/uploads/vdai/documents/files/Republic%20of%20Lithuania%20Law%20on%20legal%20protection%20of%20personal%20data%202018%20Non-Official%20Translation%2001_12_2021.pdf) and other Lithuanian national law regulating the processing of personal data.

For Poland, “Applicable Data Protection Law” also includes the Polish Personal Data Protection Act of 10 May 2018 (Journal od Laws of 2019, Item 1781 – uniform text; “**PDPA**”).

For Portugal, “Applicable Data Protection Law” also includes Law No. 58/2019 of 8 August 2019 implementing the GDPR in Portugal and Law No. 41/2004 of 18 August 2004 on Data Protection and Privacy in the Electronic Communications. For Spain, “Applicable Data Protection Law” would also

include, if applicable under EU principles, Spanish Fundamental Act 3/2018 on the Protection of Personal Data and the Guarantee of Digital Rights "NLOPD".

For Romania, "Applicable Data Protection Law" includes Law No 190 of July 18, 2018 on the measures implementing Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), Law no. 506 of November 17, 2004 on the processing of personal data and the protection of privacy in the electronic communications sector and all Decisions issued by The National Supervisory Authority For Personal Data Processing.

For Slovakia, "Applicable Data Protection Law" also includes Act No. 18/2018 Coll. on the Protection of Personal Data and on Amendments and Additions to Certain Acts, as amended ("SDPA").

For Slovenia, "Applicable Data Protection Law" also includes the Personal Data Protection Act (ZVOP-2), Official Gazette of the Republic of Slovenia no. 163/22 and the Electronic Communications Act (ZEKom-2), Official Gazette of the Republic of Slovenia no. 130/22 with subsequent changes.

For Sweden, "Applicable Data Protection Law" also includes Law (2018:218) with provisions complementing the General Data Protection Regulation.

Unless otherwise stated, terms defined by law, such as "**personal data**", "**processing**" and "**data controller**" shall in this Privacy Notice have the same meaning as in the Applicable Data Protection Law.

Accordingly, "**personal data**" means any information relating to an identified or identifiable natural person ('**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.

The term "**processing**" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

A short description of TCS' processing of personal data

TCS processes your personal data as you are a representative or an employee of a customer to TCS. The personal data that we process is to a great extent

and generally collected from yourself, such as contact information. In cases where we furthermore process personal data about you from Third Party or other sources e.g. the charging sessions, we will provide transparency in this regard.

We process your personal data for various purposes, including for us to be able to offer your employer the TCS eMSP Service, and to the extent necessary to establish, exercise and defend legal claims.

We process your personal data during the time your employer has a contractual relationship with us about our supply of the TCS eMSP Service. However, we might process personal data during a longer period of time, in order to e.g. comply with legal obligations to which we are subject.

Data Controller

TCS is controller for the processing of personal data that is described in this Privacy Notice. For further contact details, please see below in this Privacy Notice.

Information about the categories of personal data processed

Categories of personal data	Meaning	Examples of personal data processed
Driver identification data	Data that can identify you as a driver of a specific vehicle when you use the Driver App provided by a Brand Partner* of TCS to manage a charging session.	<ul style="list-style-type: none"> • Name • Login credentials • Driver ID (from the Driver App of the respective TCS Brand Partner*) • Email-address • Telephone number • Information about employer • User ID • Preferred language
Administrator identification data	Data about users that act as administrators for the eMSP Service	<ul style="list-style-type: none"> • Name • Login credentials • Customer ID • Email-address • Telephone number • Information about employer

Charging data	Data about the charging sessions	<ul style="list-style-type: none"> • RFID card utilized to identify driver when starting charging session • Driver identification data utilized to identify driver when starting charging sessions via the Driver App of the Brand Partner • Start time of the charging sessions • Stop time of the charging session • Amount of electricity charged • Cost for electricity charged • Charging station where charging occurred (EVSE ID, station label, location of the station, Charging Point Operator (CPO)) • Alias as additional text field that is printed on the card. • The physically printed id on the RFID card. • The digital unique identifier given to the RFID card. •
Information about your location	Data about your location if you submit a support ticket or similar message about a non-functioning charging station	<ul style="list-style-type: none"> • Location data
User feedback	Data that you provide us with when you provide us with feedback regarding your experience with the TCS eMSP Service.	<ul style="list-style-type: none"> • User role, e.g. driver • Feedback messages

		<ul style="list-style-type: none"> • Questionnaire replies • Feedback rating
Support information related	Data collected in the context of contacting the support center or using the support offering otherwise	<ul style="list-style-type: none"> • Name, email address, phone/contact number • Incident description • Incident ticket number •

* **Brand Partner is Scania CV AB in the event of using the Scania Driver App, Brand Partner is MAN Truck & Bus SE when using the MAN Driver App**

From where do we collect personal data?

We collect your personal data from:

Yourself

We process the personal data that you provide us with, for example in your communication with us or through your use of our service, such as identification data, provided by you when subscribing to the eMSP Service. Further, we collect personal data when you interact with us during your receipt of the TCS eMSP Service, such as charging data and user feedback.

Your employer

We process personal data that your employer provides us with, such as user identification data.

Charge point operators

We process personal data that the charge point owner/operator provide us with when you charge your vehicle.

Other entities in the TRATON group

We process personal data that we receive from other entities in the TRATON group, e.g. from Brand Partners, for example contact information from the Scania group that you submit when creating your MyScania account, or from the TRATON group when creating your RIO Platform account.

When and why do we process your personal data?

Below you will find information about for what purposes we process your personal data, the legal bases for the processing and for how long we store your personal data (subject to supplementary legal retention obligations).

To administer the setup of the TCS eMSP Service

We process your personal data in order to administer the connection between, for drivers, the eMSP tile in your Driver App provided by the Brand Partner* or, for administrators, the eMSP tile in the Online Platform** that is provided by the platform provider to enable TCS to provide the eMSP Services.

** Online Platform for eMSP Services with Scania as enabling Business Partner of TCS is the MyScania Portal operated by Scania AB and Online Platform with MAN as enabling Business Partner of TCS is the RIO Platform operated by TB Digital Services GmbH.

In this context, we wish to inform you that the Online Platform and the Driver App are services provided by certain other entities of the TRATON group and that those other entities may process your personal data in addition to what is set out in this Privacy Notice. The applicable Legal Notice and Privacy Statement governing the Online Platform and the Driver Application are accessible on their respective official websites.

Categories of personal data

- Driver identification data
- Administrator identification data

Legal basis

Legitimate interest, GDPR and UK GDPR art. 6 (1) (f) or equivalent provisions in other Applicable Data Protection Law – the processing of your personal data is necessary for the purposes of our legitimate interest in being able to connect the TCS eMSP service to your Driver App or the Online Platform as a part of our offering of the eMSP Service.

Retention period: The personal data will be retained for this purpose as long as your employer has a contractual relationship with us about our supply of the TCS eMSP Service. In certain instances your personal data may be retained for a longer period of time due to legal obligations.

To provide the TCS eMSP Service

We process your personal data as a driver or an administrator in order to be able to provide the TCS eMSP Service, e.g. in enabling you to start and stop charging sessions at connected charging stations, to pay for the charging sessions and for fleet management purposes.

Categories of personal data

- Driver identification data
- Administrator identification data
- Charging data

Legal basis

Legitimate interest, GDPR and UK GDPR art. 6 (1) (f) or equivalent provisions in other Applicable Data Protection Law – the processing of your personal data is necessary for the purposes of our legitimate interest to be able to provide the TCS eMSP Service to you as a driver of your employer's vehicle or as an administrator managing your employer's fleet of vehicles.

Retention period: The personal data will be retained for this purpose as long as your employer has a contractual relationship with us about our supply of the TCS eMSP Service. In certain instances your personal data may be retained for a longer period of time due to legal obligations.

To administer the payment of the electricity purchased

We process your personal data in order for us to be able to administer your employer's payment for the electricity purchased by you when charging the vehicle.

Categories of personal data

- Driver identification data
- Charging data

Legal basis

Legitimate interest, GDPR and UK GDPR art. 6 (1) (f) or equivalent provisions in other Applicable Data Protection Law – the processing of your personal data is necessary for the purposes of our legitimate interest in handling invoicing and payment for the electricity purchased as a part of the TCS eMSP Service.

Retention period: The personal data will be retained for this purpose as long as your employer has a contractual relationship with us about our supply of the TCS eMSP Service. In certain instances your personal data may be retained for a longer period of time due to legal obligations.

Customer support

We process your personal data in order for us to be able to provide you with customer support, should you have any issue related to the TCS eMSP Service.

Categories of personal data

- Driver identification data
- Administrator identification data
- Information about your location
- Charging data
- Support contact

Legal basis

Legitimate interest, GDPR and UK GDPR art. 6 (1) (f) or equivalent provisions in other Applicable Data Protection Law – the processing of your personal data is necessary for the purposes of our legitimate interest in providing you with customer support as needed when you utilize the TCS eMSP Service.

Retention period: The personal data will be retained for this purpose for the time necessary to provide you with customer support. In certain instances your personal data may be retained for a longer period of time due to legal obligations.

Use of AI in Customer Support

To improve our service and our experience, we use AI-based voice translation technology during customer support calls. This processing is limited to service delivery and workflow processes and does not involve profiling or automated decision-making. If personal data will be processed we follow Data Protection Law principles of lawfulness, fairness, and data minimization, and comply with applicable Data Protection Law and Regulation (EU) 2024/1689 on Artificial Intelligence (EU AI Act). Our partner Teleperformance Germany S.a.r.l & Co. KG, located at Heinrich-Hertz-Str. 4, 44227 Dortmund, Germany, provides these services under strict data protection agreements. Your rights under GDPR—including access, rectification, and erasure—remain fully protected.

Analysing and developing the TCS eMSP Service, evaluating service usage and improving user experience

We process your personal data in order to analyse and develop the TCS eMSP Service, to evaluate the use of the service and to improve our user experience.

Categories of personal data

- Driver identification data
- Administrator identification data

- Charging data
- User feedback

Legal basis

Legitimate interest, GDPR and UK GDPR art. 6 (1) (f) or equivalent provisions in other Applicable Data Protection Law – the processing of your personal data is necessary for the purposes of our legitimate interest in developing the TCS eMSP Service based on your feedback.

Retention period: The personal data will be retained for this purpose as long as your employer has a contractual relationship with us about our supply of the TCS eMSP Service. In certain instances your personal data may be retained for a longer period of time due to legal obligations.

Fulfil legal obligations

We process your personal data in order to fulfil legal obligations relevant to us, such as accounting obligations.

Categories of personal data

- Driver identification data
- Administrator identification data
- Information about your location
- Charging data
- User feedback

Legal basis

Legal obligation, GDPR and UK GDPR art. 6 (1) (c) or equivalent provisions in other Applicable Data Protection Law – the processing is necessary to comply with a legal obligation to which we are subject.

Retention period: The personal data will be retained for the time necessary to comply with our legal obligations. Accounting information will be retained during such periods of time as may be required for bookkeeping purposes in the country where transactions took place to comply with legal obligations under, among other legislation, the bookkeeping legislation applicable in the country in which you transact with us.

In Belgium, accounting information will be retained for 7 years from 1 January following the end of the accounting year for bookkeeping purposes to comply with legal obligations under, among other legislation, the Belgian Code of Economic Law.

In Bulgaria, accounting information will be retained for 10 years from 1 January following the end of the accounting year for bookkeeping purposes to comply

with legal obligations under, among other legislation, the Bulgarian Accountancy Act.

In Croatia, accounting information will be retained for a period ranging from 6 years until permanently, starting from the end of the relevant accounting year for bookkeeping purposes to comply with legal obligations under, among other legislation, the Croatian Accounting Act (*Zakon o računovodstvu*).

In Cyprus, accounting information will be retained for 7 years from the end of the tax year to which they refer for bookkeeping purposes to comply with legal obligations, under sections 30(2) and 30(3) of the Law 4/1978 on Assessment and Collection of Taxes; records and evidences of all expenses of entities subject to VAT will be retained for a period of 7 years from the date of the expense to comply with legal obligations, under section 5(3) of the Law 95(I)/2000 on Value Added Tax.

In Czech Republic, accounting information related to wages shall be retained for 45 years from termination of respective employee for bookkeeping purposes to comply with legal obligations under, among other legislation, with Section 35a paragraph 4 of the Act No. 582/1991 Coll. on the organization and implementation of social security, considering these records as a “necessary document”.

In Estonia, accounting information will be retained for 7 years from the end of the relevant accounting year for bookkeeping purposes to comply with legal obligations under, among other legislation, the Estonian Accounting Act (*Raamatupidamise seadus*) and the Estonian Taxation Act (*Maksukorralduse seadus*).

In Germany, the retention period generally ranges from 6 to 10 years, depending on the type of document. For example, accounting records are required to be retained for 10 years from the end of the relevant financial year for bookkeeping purposes, in order to comply with legal obligations under the German Commercial Code (*Handelsgesetzbuch, HGB*) and the Tax Code (*Abgabenordnung, AO*) In Finland, accounting information will be retained for 10 years from the end of the relevant accounting year for bookkeeping purposes to comply with legal obligations under, among other legislation, the Finnish Accounting Act (*Kirjanpitolaki*).

In France, accounting information will be retained for 10 years from the end of the relevant accounting year for bookkeeping purposes to comply with legal obligations notably Article L.123-22 of the French Commercial Code (*Code de commerce*).

In Sweden, accounting information will be retained for 7 years from 1 January following the end of the accounting year for bookkeeping purposes to comply with legal obligations under, among other legislation, the Swedish Accounting Act.

In Hungary, generally accounting information will be retained for 8 years for bookkeeping purposes to comply with legal obligations under, among other legislation, Act C of 2000 on Accounting.

In Iceland, accounting information will be retained for 7 years from the end of the relevant accounting year for bookkeeping purposes to comply with legal obligations under the Icelandic Accounting Act No. 145/1994.

In Ireland, accounting information will be held for 6 years from the end of the relevant accounting period for bookkeeping purposes to comply with legal obligations to which TCS is subject, including in accordance with Section 285 of the Companies Act 2014. In some instances we may hold the data for 7 years to enable us to defend claims brought against us, in accordance with the Statute of Limitation Act 1957.

In Italy, accounting information will be retained for 10 years from the end of the relevant accounting year for bookkeeping purposes to comply with legal obligations, notably Article 2020 of the Italian Civil Code.

In Latvia, accounting information will be retained for 10 years from the listed date of the bookkeeping document, invoice or related documentation for bookkeeping purposes to comply with legal obligations, notably the Latvian Accounting Law.

In Lithuania, accounting information will be retained for 10 years from the end of the relevant accounting year for bookkeeping purposes to comply with legal obligations under, among other legislation, the Lithuanian Index of Terms for Storage of General Documents.

In Poland, records and information documenting revenues received, including accounts receivable records, cash receipts, billing records, etc., may be retained for 5 years from the end of the calendar year in which the document was issued or in which the payment of the tax was due in order to comply with legal obligations under, among other legislation the Accounting Act of 29 September 1994 and Tax Ordinance of 29 August 1997.

In Portugal, accounting information will be retained for 10 years from the end of the relevant accounting year for bookkeeping purposes to comply with legal obligations under, among other legislation, the Portuguese Commercial Code and Tax codes.

In Romania, as a rule, accounting information will be retained 5 years from 1st July of the year following the end of the financial year in which the documents containing account information were prepared for bookkeeping, to comply with legal obligations.

In Slovakia, accounting information will be retained for 10 years from the end of the relevant accounting year for bookkeeping purposes to comply with legal obligations under, among other regulations, the Slovak Accounting Act.

In Slovenia, accounting information will be retained for 10 years from the end of the relevant accounting year for bookkeeping purposes to comply with legal obligations under, among other legislation, the Slovenian Companies Act (*Zakon o gospodarskih družbah – ZGD-1*), Tax Procedure Act (*Zakon o davčnem postopku – ZdavP-2*), Value Added Tax Act (*Zakon o davku na dodano vrednost – ZDDV-1*) and the Accounting Act (*Zakon o računovodstvu – ZR*).

In Spain, the relevant data will be retained for 6 years from the date they were generated / last recorded for purpose of complying with legal obligations and for defending and filing lawsuits and regulatory complaints, under, among other legislation, the Spanish Code of Commerce (Article 30) and the Spanish Civil Code (Article 1964.2).

Establish, exercise and defend legal claims

We process your personal data in order to establish, exercise and defend legal claims, e.g. in connection with a dispute or judicial process.

Categories of personal data

- Driver identification data
- Administrator identification data
- Information about your location
- Charging data
- User feedback

Legal basis

Legitimate interest, GDPR and UK GDPR art. 6 (1) (f) or equivalent provisions in other Applicable Data Protection Law – the processing of your personal data is necessary for the purposes of our legitimate interest in establishing, exercising and defending legal claims, e.g. in connection with a dispute or other legal proceedings.

Retention period: Your personal data will be retained for the relevant purpose during the time when it is necessary in order to handle and respond to the legal claim, or during the applicable statutory limitation periods. In certain instances your personal data may be retained for a longer period of time due to legal obligations.

In Bulgaria, the data can be kept up to 5 years from the end of the contractual relationship with the client.

In Cyprus, the relevant data will be retained for 6 years from the date on which the grounds of the legal claim is based, for filing or defending lawsuits in relation to contractual agreements, under section 7(1) of Law 66(I)/2012 on Limitation of Legal Proceedings.

In France, the data can be kept up to 5 years from the end of the contractual relationship with the client.

In Hungary, the general statutory limitation period is 5 years, under Act V of 2013 on the Civil Code.

In Slovakia, the relevant data will be retained during the limitation period stated by the Slovak Civil Code or Slovak Commercial Code for exercising the claim. In general, the retention period of 3 or 4 years since the claim arose, depending on the nature of the claim and applicability of Slovak Civil Code or Slovak Commercial Code, will apply. In addition, depending on the nature of the particular claim, the different limitation period prescribed by Slovak law may apply and in that scenario the relevant data will be retained during all this statutory limitation period.

In Slovenia, the data can be kept up to 5 years from the end of the contractual relationship with the client.

In Spain, the relevant data will be retained for 6 years from the date they were generated / last recorded for purpose of complying with legal obligations and for defending and filing lawsuits and regulatory complaints, under, among other legislation, the Spanish Code of Commerce (Article 30) and the Spanish Civil Code (Article 1964.2).

Enable contemplated or actual business changes

We may process your personal data in anonymized or pseudonymized form in order to enable contemplated or actual business changes, e.g. sale or merger of the business or investments in or by our business.

Categories of personal data

- Driver identification data
- Administrator identification data
- Information about your location
- Charging data
- User feedback

Legal basis

Legitimate interest, GDPR and UK GDPR art. 6 (1) (f) or equivalent provisions in other Applicable Data Protection Law – the processing of your personal data is necessary for the purposes of our legitimate interest in conducting and effectively executing business changes.

Retention period: Your personal data will be retained for the relevant purpose during the time when it is necessary in order to enable contemplated or actual business changes.

Recipients with whom TCS may share your personal data

For the purposes set out in this Privacy Notice, we may transfer your personal data in anonymized or pseudonymized to our service providers and business partners, e.g. providers of IT services or consultants. These parties will generally act as processors relating to the processing of personal data, which means that they are contractually obliged to process your personal data only on behalf of and in accordance with our instructions. These service providers and business partners include charging partners, card providers, customer service providers, e-roaming providers and invoicing service providers.

We may also share personal data with other recipients, in which case both we and the recipient will act as data controllers, in accordance with the below:

Recipient	Purpose	Legal basis
Other TRATON group companies	We may share your personal data with the members of the TRATON Group for the purposes set out above. For example, we share driver identification data utilized to identify driver when starting charging sessions via the Scania Driver App with the Scania group (with respect to Scania vehicles) or via the MAN Driver App with the MAN group (with respect to MAN vehicles).), customer relationship purposes, service utilization analysis purposes, improving the service purposes and consulting purposes	Legitimate interest, GDPR art. 6 (1) (f). The processing is necessary for the purposes of our legitimate interest pursued as set out above.
Professional advisers, such as auditors and attorneys	We may share your personal data with professional advisers, acting as controllers, for	Legitimate interest, GDPR art. 6 (1) (f). The processing is necessary for the purposes of our

	the purposes listed above in this Privacy Notice.	legitimate interest in ensuring in particular, regulatory compliance, obtaining legal advice, fulfilling audit requirements, defending legal claims, and maintaining the overall legal and financial standing of the company.
Authorities (e.g. law enforcement, tax authorities) and external advisors	To fulfil any legal obligations to which we are subject, for example in connection with requests from authorities or other legal requirements.	Legal obligation, GDPR and UK GDPR art. 6 (1) (c) or equivalent provisions in other Applicable Data Protection Law. The processing of personal data is necessary for compliance with legal obligations to which we are subject.
Potential buyers and sellers, investors and external advisors/other parties involved, licensees, licensors, collaboration partners and representatives thereof	To enable contemplated or actual business changes, e.g. sale or merger of the business or investments in general.	Legitimate interest, GDPR and UK GDPR art. 6 (1) (f) or equivalent provisions in other Applicable Data Protection Law, to the extent that the processing of data in personal form is necessary for the purposes of our legitimate interest in conducting and executing business changes.

Where do we process your personal data?

Should TCS transfer your personal data processed (a) under the GDPR or other Applicable Data Protection Law to a recipient located in countries outside the EU/EEA; or (b) under the UK GDPR to a recipient located outside the UK (each a "third country"), such transfer will only take place where an adequate level of protection is ensured (a) in the case of the GDPR, in accordance with a decision by the European Commission or other competent data protection authorities; or (b) in accordance with the adequacy regulations referred to in UK GDPR art. 45 (1). Alternatively, we will ensure that appropriate safeguards have been implemented (in particular those provided for (a) in the case of the GDPR in the European Commission's standard contractual clauses and supplementary measures, if necessary; and (b) in the case of the UK GDPR in the international data transfer agreement or the international data transfer addendum to the European Commission's standard

contractual clauses). Where deemed necessary, such appropriate safeguards will be complemented by supplementary measures for ensuring an essentially equivalent level of data protection to that found under the GDPR or other Applicable Data Protection Law / UK GDPR, as applicable.

TCS may transfer your personal data to India in anonymized or pseudonymized (a country whose level of protection of privacy rights is not equivalent to the one applied within the European Union) using data processors.

Under the GDPR, other Applicable Data Protection Law and the UK GDPR, you have the right to, upon request, receive a copy of documentation that demonstrates that the appropriate safeguards have been implemented in order to protect your personal data when transferred to a third country. Please contact us via the contact information below to obtain such documentation.

Your rights under the GDPR or other Applicable Data Protection Law

In connection with our processing of your personal data under the GDPR, other Applicable Data Protection Law or the UK GDPR, you have the rights listed below. If you want to exercise any such right, please contact us via the contact details listed below.

The right to access

You can request confirmation of whether or not your personal data is being processed and, if it is being processed, request access to your personal data and additional information such as the purpose of the processing. You also have the right to receive a copy of the personal data that is processed. If the request is submitted electronically, the information will also be obtained in a commonly used electronic form unless you request otherwise.

The right to access does not apply to personal data that we are not allowed to disclose to you pursuant to an act or other statute or a decision issued pursuant to a statute. Furthermore, the right to access does not apply to personal data that would have been subject to secrecy at a public authority under applicable law.

For Portugal, besides the cases where we are not legally allowed to disclose the personal data to you, the right to access also does not apply where we are subject to a duty of secrecy that can be invoked against you.

Right to rectification

If you discover that personal data relating to you is inaccurate, incomplete or incorrect, you have the right to have your personal data rectified or completed.

Right to object

You can, at any time, object to processing of your personal data if it is based on a legitimate interest, on grounds relating to your specific situation, or if the processing takes place for direct marketing purposes. Upon such an objection, we are obliged to cease the processing, unless we can demonstrate compelling legitimate grounds for continuing the processing and those grounds override your interests, rights and freedoms. We may also continue processing that is necessary to establish, exercise and defend legal claims. Processing for direct marketing purposes will, however, always be ceased upon your objection.

If you object to the processing of your personal data, you have the right to request restriction of processing pending our verification of whether we may continue to process it as set out below (see below Restriction of processing).

If, upon your objection, we no longer have the right to process your personal data, you have the right to have the personal data erased as described below (see below Right to erasure).

Right to erasure

You may have your personal data deleted under the following circumstances (subject to other legal obligations to retain your data):

- If the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed;
- If the processing of the personal data can only be carried out based on your consent, and you withdraw such consent;
- If you object to the processing, provided that our processing is based on legitimate interest and (i) there are no overriding legitimate grounds for the processing, or (ii) if the processing in question is carried out for direct marketing purposes:
- If your personal data has been unlawfully processed; and
- If your personal data must be erased for compliance with a legal obligation (a) in the case of the GDPR, in Union or Member State law; and (b) in the case of the UK GDPR, in domestic law, to which we are subject.

The right to erasure does not apply to the extent that the processing is necessary for the exercise of the right to freedom of expression and information; for compliance with a legal obligation which requires the processing; or for the establishment, exercise or defense of legal claims.

Right to restriction

Under the following circumstances, you may request that we restrict the processing of your personal data to solely involve the storage of your personal data:

- If you contest the accuracy of the personal data, we will restrict the processing for the time required to verify its accuracy.
- If the processing is unlawful and you oppose the erasure of the personal data and request that its use is instead restricted.
- If we no longer need the personal data for the purposes of the processing, but they are required by you to be able to establish, exercise or defend legal claims.
- If you have objected to processing, you have a right to restriction pending verification of whether our legitimate grounds override your legitimate reasons.

We may, however, still use your personal data for the establishment, exercise or defense of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest (a) in case of the GDPR, of the Union or a Member State; or (b) in case of the UK GDPR, the United Kingdom.

Withdrawal of consent

To the extent that the processing of personal data is based on your consent, you have the right to withdraw your consent to the processing of personal data at any time. This withdrawal will not affect the lawfulness of any processing carried out before its withdrawal. If there is no other legal basis for the processing, you have the right to have the relevant personal data deleted as described above (see above **Right to erasure**).

Right to Data portability

Unless it adversely would affect the rights and freedoms of others, you have the right to request a structured, commonly used and machine-readable copy of the personal data processed on the basis of your consent or where the processing is necessary for the performance of a contract with you, and where personal data has been provided by you, and to request that the information is transferred to another data controller (if possible).

Digital legacy (France, Italy, and Portugal only)

If you are a French data subject, you have the right to set out instructions (general or specific) about what happens to your personal data after your death.

If you are a data subject located in Italy, you have the right to provide us with instructions to prohibit your heirs from exercising any of the rights listed in this section on your personal data after your death.

If you are a Portuguese resident data subject, in case of certain personal data (i.e., special categories, private life, image and communications data) you have the right to appoint a person to exercise your data protection rights after your death or to set out instructions prohibiting the exercise of such rights after your death. **Right to lodge a complaint with a supervisory authority**

Please contact us with questions or complaints regarding our processing of your personal data. You also always have the right to lodge a complaint with a data protection supervisory authority, in particular in the Member State of your habitual residence, place of work or of an alleged infringement of the GDPR regarding the processing of your personal data . For more information on how to contact your local data protection supervisory authority, please visit

<https://www.dsb.gv.at> (for Austria)

www.dataprotectionauthority.be (for Belgium); Other contact details of the Belgian DPA: Belgian Data Protection Authority, Address: Drukpersstraat 35, 1000 Brussels, Belgium; Tel. +32 2 274 48 00; Email: contact@apd-gba.be

<https://cpdp.bg/> (for Bulgaria)

www.azop.hr (for Croatia)

<https://www.dataprotection.gov.cy/> (for Cyprus)

<https://uouu.gov.cz/en> (for the Czech Republic)

<https://www.datatilsynet.dk/english> (for Denmark)

<https://www.aki.ee/> (for Estonia)

<https://tietosuoja.fi> (for Finland)

<https://www.cnil.fr> (for France)

<https://www.bfdi.bund.de/DE/Service/Anschriften/Laender/Laender-node.html> (in Germany, there are 16 different supervisory authorities on a regional level; for a comprehensive list of these authorities, please refer to the provided link.)

<https://www.naih.hu/> (for Hungary), other contact details of the Hungarian DPA: National Authority for Data Protection and Freedom of Information (“NAIH”), address: 1055 Budapest, Falk Miksa utca 9-11., Hungary, phone: +36 (1) 391-1400, e-mail: ugyfelszolgalat@naih.hu

<https://dataprotection.ie/en> (for Ireland)

<https://www.personuvernd.is/> (for Iceland)

<https://www.garanteprivacy.it/> (for Italy)

<https://www.dvi.gov.lv> (for Latvia)

<https://vdai.lrv.lt/lt/> (for Lithuania)

<https://cnpd.public.lu/> (for Luxembourg)

<https://autoriteitpersoonsgegevens.nl/> (for the Netherlands)

www.datatilsynet.no (for Norway)

<https://www.uodo.gov.pl/> (for Poland)

<https://www.cnpd.pt/> (for Portugal)

<https://www.dataprotection.ro/> (for Romania)

<https://dataprotection.gov.sk/sk/> (for Slovakia)

<https://www.ip-rs.si/> (for Slovenia)

www.aepd.es (for Spain)

<https://www.imy.se/> (for Sweden)

<https://www.edoeb.admin.ch/edoeb/de/home.html> (for Switzerland)

<https://ico.org.uk/> (for the United Kingdom)

Updates to this Privacy Notice

The Privacy Notice can be updated from time to time, and we encourage you to read it now and then. Where appropriate, we will also inform you of changes that we make.

Contact us

If you have any questions regarding the processing of your personal data or if you wish to exercise any of your rights pursuant to applicable data protection legislation, please contact us by using the contact details below.

To contact TCS' data protection department, including our data protection officer, please visit the section Contact at our website [Information on data protection | TRATON](#).