

Data Access & Sharing Terms

Key Information Summary

This product generates data as part of its normal operation. You (the User) have the following rights under the EU Data Act:

1. What data are generated

The device generates operational, configuration, security, and activity data. A full list is available in the Terms (Sections 2.1 and 2.2).

Data include, for example: lock/unlock events, device state, configuration settings, and diagnostic logs.

2. Your rights

You can:

- access all data that are “readily available” from the device or software;
- request the data in a structured, machine-readable format;
- request that data be shared with a third party of your choice;
- choose the frequency (one-time, continuous, or real-time, where technically possible);
- withdraw permission for Tedee to use your data in certain cases.

The respective form is provided in Appendix 1.

3. What Tedee may do with the data

Tedee uses non-personal data only to:

- provide and improve the service,
- maintain safety and security,
- generate aggregated, anonymised insights.

Tedee does not use data to profile your financial situation, business secrets or behaviour in a way that harms you.

4. Sharing data with third parties

At your request, Tedee will share the data with a third party (not a DMA gatekeeper) free of charge, and with necessary metadata.

The respective form is provided in Appendix 2.

5. Fees

If you are a micro, small, or medium enterprise, Tedee does not charge any compensation for making data available.

6. Restrictions

Tedee may temporarily suspend access only to protect security, trade secrets, or rights of others, and will inform you unless this would compromise safety

1. Introduction and purpose of these Terms

- 1.1. Please read these Terms carefully before using Tedee Products or related services.
- 1.2. They explain your rights and our responsibilities when it comes to data generated by your Tedee device, in particular how Tedee processes and makes that data available under the EU Data Act.
- 1.3. These Terms set out the rules for how Tedee handles and shares your non-personal data in accordance with Regulation (EU) 2023/2854 of the European Parliament and of the Council - the EU Data Act.
- 1.4. Tedee sp. z o. o., based in Warsaw, Poland (Karola Bohdanowicza 21/57, 02-127 Warsaw), registered under number 0000712451 (District Court for the Capital City of Warsaw, 12th Commercial Division of the National Court Register), VAT ID 7010795542, REGON 369188621, is the Data Holder under these Terms.
- 1.5. You are the User, meaning the person who owns or uses one or more of the following:
 - a) connected product(s) available for sale at <https://tedee.com/> , including but not limited to (the ‘**Product**’):
 - Tedee PRO;
 - Tedee GO;
 - Tedee Bridge;
 - Tedee Keypad;
 - Tedee Switch;
 - Tedee Dry Contact;
 - Tedee Door Sensor (jointly ‘**Tedee Devices**’)

b) related service(s) made available for use by Tedee, including but not limited to (the ‘**Related Service(s)**’):

- Tedee App
- Tedee API
- Tedee Smart Check-in (jointly ‘**Tedee Software**’)

1.6.By accepting these Terms of Use You declare that you are either the owner of the Product or contractually entitled to use the Product under a rent, lease or similar contract and/or to receive the Related Service(s) under a service contract.

2. Data covered by these Terms

2.1.The data covered by these Terms (the “Data”) include all readily available Product Data and Related Services Data as defined in the EU Data Act.

2.2.If new types of data become available to you during the use of Tedee Products or related services, this list will be updated to reflect those additions.

2.3.Tedee Devices

Data Type & Format	Description	Purpose	Approximate yearly volume	Data generated in real time (Y/N)	Data storage location (device, remote server)	Data retention period	How to access the Data
Tedee Lock Activities	All device-generated events: lock/unlock actions,	Provide a security audit trail and access	2MB	Y	Device	Until factory reset or memory	Tedee App or API

	door events, keypad triggers, dry-contact impulses, auto-lock triggers; with timestamps, method, and user identity/PIN alias.	transparency.				limit	
Tedee Device Configuration	Auto-lock settings, pull-spring/latch settings, button behavior, paired accessories, alert settings, Matter pairing data.	Enable customizable device behaviour and integrations.	10KB	N	Device	Until factory reset	Tedee App or API
Tedee Device States	Realtime functional state: lock position, door status, battery level, charging status, connectivity, Matter status.	Display current state, run automation, and support integrations.	1KB	Y	Device	Until power off	Tedee App or API

Tedee Device Security Data	Cryptographic key pairs (device-only), public certificates, revocation list metadata, secure channel parameters	Ensure secure communication and device authentication	3KB	N	Device	Persistent or until factory reset	No
PIN Code Authorization Data	PINs stored on the; metadata: PIN alias, schedule, validity.	Allow keypad-based access control with scheduling and auditing	10KB	N	Device	Persistent until removed by user.	App or API
Fingerprint Authorization Data	Fingerprint biometric templates stored only inside the fingerprint module. Device store metadata: slot index, custom label, schedule. Templates cannot	Provide biometric access to the device while protecting biometric privacy.	2KB	N	Device	Persistent until removed on device.	User can see list of enrolled fingerprints (labels) in app and remove them. Raw fingerprint data is never accessible

be exported or read.

Tedee Bridge Authorization & Network Data	WiFi SSID/password, MQTT credentials.	Allow Bridge to connect to cloud securely.	3KB	N	Device	Persistent until reset.	Not visible; user can only reconfigure via setup flow
Device Internal Logs	Crash reports, error flags, watchdog resets, firmware debug logs	Firmware diagnostics and troubleshooting	50KB	Y	Device		App

2.4.Tedee Software

Data Type & Description		Purpose	Approximate yearly data volume	Data generated in real time (Y/N)	Data storage location (device, remote server)	Data retention period	How to access the Data
Tedee App Authorization Data	OAuth tokens, refresh tokens, app certificates	Enable secure login and allow app to communicate with backend and devices	10KB	N	Device	Until logout/token expiry/uninstall.	Not directly visible; managed via logout/account settings
Tedee App Cached Device Data	Locally cached list of user devices, settings, accessories, and partial access rights.	Improve performance, enable offline mode, reduce API calls.	200KB	Y	Local storage on mobile device.	Until logout	Visible indirectly via device list and settings UI.
Tedee App Firmware Storage	Temporary firmware files downloaded for device updates.	Deliver firmware updates to the	4MB	N	Local temporary storage on	Deleted immediately	Not visible to user.

(OTA)		device via BLE.				mobile.	after update.	
Tedee App User Data	Logged-in user identity: email, profile data, selected language, app preferences.	Personalize the user experience and authenticate requests.	10KB	N	Device	Persistent until account deletion/logout		
Tedee App Logs	Debug logs: BLE scans, connection events, errors, crashes, performance traces.	Diagnostics and support troubleshooting.	10MB	Y	Local mobile storage	Short-lived up to 3 days or until memory capacity reached	Export via App	
Tedee App Last Auto-Unlock Status	Result and reasoning of the last auto-unlock attempt: geofence checks, WiFi verification, motion state, BLE discovery, timing steps	Allow user to understand why auto-unlock succeeded or failed	10KB	Y	Local mobile storage	Temporary (most recent event only).	Visible in app under Auto-Unlock → Last Status	
Device configuration data	Configuration data of Tedee devices	Managing devices	25KB		Until account deletion	Yes	API	
Access	Who can access the Tedee	Access control	100KB		Until	Yes	API	

Control Data	device, access level, schedules				account deletion			
Certificate & Crypto metadata	E2E certificates, revocation metadata	Access Control and security	2KB		Until account deletion	No		No
Device Activities	All lock activities like lock/unlock/trigger events, timestamps, source	Historical log of access for auditing	10MB		Until account deletion	Yes		API
User configuration	User configuration like notification preferences, app configuration,	User system personalization	10KB		Until account deletion	Yes		API
Registered mobile devices	List of mobile devices used by user together with device name and operation system	Security and push notifications control	5KB		Until account deletion	Yes		API
Access Links	Generated access links with access details	Managin access for guests	150KB		Until account deletion	Yes		API

Organization configuration	Configured organizations by user with organization name, users, groups, assigned devices	Managing organization	20KB		Until account deletion	Yes	API
User account Data	Authentication email, display name	Identity,	Authentication and security	10KB	Until account deletion	Yes	API
Rental Services	Configured smart rental services and linked account	Authentication		15KB	Until account deletion	No	API
Rental Bookings	Bookings configured services	synced smart rental	Showing bookings and enabling automations	300KB	Until account deletion	No	API
Rental Listings	Listings configured services	synced smart rental	Showing bookings and enabling automations	20KB	Until account deletion	No	API

API Requests	Log of API requests sent to our system	Security, auditing and rate limits	30MB	year	No	No
Device state	Current Tedee device connection/battery/position state	Automations and remote device control	2KB	Until account deletion	Yes	API

Legal grounds for Tedee Software data processing

2.5.Data from the Tedee Software are processed from the moment you create a user account in the Tedee App, in accordance with the Terms and Conditions available at www.tedee.com/legal, and continue to be processed until your user account is deleted.

3. Data use and sharing by Tedee

3.1.Purposes of data use

Tedee processes and uses non-personal data only for the purposes agreed with you, including:

- a) providing and performing the agreement with you - for example, issuing invoices, generating reports, or offering analytical insights;
- b) offering customer support, warranty or guarantee services, and handling claims or issues related to the Product or related services;
- c) monitoring, maintaining, and improving the safety, security, and performance of Tedee Products and related services;

- d) developing and improving Tedee's products and services, including solutions that use artificial intelligence (AI), either directly or with trusted partners acting on Tedee's behalf;
- e) combining or aggregating your Data with other data to create insights or derived datasets, provided that such data cannot be used to identify you or any specific information from your connected Product.

3.2. Personal data

If Tedee processes personal data, this is done only on a valid legal basis and under the conditions permitted by Regulation (EU) 2016/679 (GDPR) and, where relevant, Directive 2002/58/EC (the ePrivacy Directive).

The specific rules and legal bases for personal data processing are described in the Privacy Policy available at www.tedee.com/legal.

3.3. Prohibited Data processing purposes

Tedee will not use the Data to analyse or draw conclusions about your financial situation, business activity, production methods, or how you use the Product or related services in any way that could negatively affect your commercial position or interests.

Tedee will use the Data only for the purposes described in these Terms and will not allow any other use.

Appropriate organisational and technical safeguards are in place to ensure that no third party, inside or outside Tedee, can use the Data in a way that breaches these Terms.

3.4. Sharing of non-personal data with third parties and use of processing services

3.4.1 Tedee may share your non-personal Data with trusted third parties only when this is necessary for the purposes described in these Terms.

Such third parties may include, for example, service providers that help Tedee operate, analyse, or improve its products and related services.

3.4.2 Furthermore, Tedee will only share your Data with third parties who agree to use the Data solely for the purpose you requested and to provide equivalent protection for your data as required by the Data Act.

3.4.3 All third parties processing the Data on Tedee's behalf laid out below act only under Tedee's instructions and are bound by contractual, organisational, and technical safeguards that ensure the Data are protected and used lawfully:

Legal Name	Scope of data shared	Purpose	Legal grounds
Third-party integrators, such a Google Home, the full list is available at: https://tedee.com/smart-home-	Tedee Devices	Integration of Tedee Devices with Google Smart Home Service	User consent granted upon integration

integrations			
--------------	--	--	--

3.5.Conditions for sharing data with third parties

3.5.1. When Tedee shares non-personal data with trusted third parties, it does so under strict contractual terms.

3.5.2. Tedee requires all such third parties to:

- a) use the Data only for the purposes allowed under these Terms and never for any other reason;
- b) not analyse or draw conclusions about your financial situation, business activity, or use of the Product or related services in any way that could harm your commercial position;
- c) apply appropriate technical and organisational security measures, considering current industry standards, potential risks of unauthorised access or loss, and the cost and effectiveness of available safeguards.

3.5.3. Tedee may also use professional data processing services - such as cloud computing, hosting, or platform services - to help achieve the purposes described in section 3.1.

3.5.4. These service providers may also rely on similar secure processing tools when working under Tedee's instructions.

3.6.Data transfers outside the European Union

- 3.6.1. If Tedee or its service providers transfer Data outside the European Union (EU) or the European Economic Area (EEA), such transfers take place only where appropriate safeguards are in place.
- 3.6.2. Tedee ensures that any international data transfer complies with applicable data protection laws, including the GDPR, for example by:
- relying on an adequacy decision of the European Commission confirming that the destination country offers an adequate level of data protection, or
 - using Standard Contractual Clauses (SCCs) or other legally approved safeguards ensuring the same level of protection as within the EU/EEA.

Whenever such transfers occur, Tedee remains responsible for ensuring that your Data is handled securely and lawfully

3.7.Data protection measures taken by Tedee

- 3.7.1. Tedee applies appropriate technical and organisational measures to protect the Data against unauthorised access, loss, alteration, or disclosure. These measures are reasonable in light of current science and technology, the potential risks to you if Data were lost or disclosed, and the cost and effectiveness of available safeguards.
- 3.7.2. Tedee's protective measures include, among others:
- a) secure data transmission using HTTPS/TLS encryption for all communication between your device, the Tedee App, and Tedee's servers;

- b) encryption at rest, using industry-standard algorithms (such as AES-256) to protect Data stored on servers and databases;
- c) secure key management through Azure Key Vault, which stores encryption keys and credentials in hardware security modules (HSMs);
- d) identity and access management controls, including Azure Active Directory, multi-factor authentication (MFA), role-based access control (RBAC), and least-privilege policies for all Tedee employees and service providers;
- e) network security mechanisms such as firewalls, network security groups, private virtual networks (VNETs), and Azure DDoS Protection to detect and block malicious traffic;
- f) continuous monitoring and threat detection through Microsoft Defender for Cloud and Azure Security Center, providing real-time alerts and automated incident response;
- g) data redundancy and backup using geo-redundant or zone-redundant storage (GRS/ZRS) to prevent data loss due to hardware failure or local incidents;
- h) logical isolation of customer data in Azure's multi-tenant environment, ensuring that your Data cannot be accessed by other tenants or clients;
- i) regular vulnerability assessments and penetration testing, performed by Tedee and certified external providers;
- j) audit logs and access records, maintained to monitor and verify authorised Data access and detect anomalies;
- k) secure data deletion procedures in line with Microsoft's hardware decommissioning standards, ensuring that deleted Data cannot be recovered;
- l) compliance with international security certifications, including ISO/IEC 27001, ISO/IEC 27018, SOC 1/2/3, and CSA STAR, verified for Microsoft Azure.

3.7.3. Tedee may implement additional appropriate technical or organisational safeguards to maintain a high level of Data security and compliance with these Terms. Tedee ensures compliance with future harmonised standards or common specifications adopted under

Art. 11(8) Data Act.

3.7.4. You agree not to alter, disable, or remove any of these technical protection measures unless Tedee gives prior written consent.

4. Data access by the User upon request

4.1.Obligation to make data available

- 4.1.1. Tedee strives to allow you for a direct device- in-device access, accessible via your end device (smartphone). However, where such access is not technically possible, i.e. you cannot export your Data yourself in accordance with Sections 2.1 and 2.2, Tedee will make your Data available upon your request.
- 4.1.2. To do so, please complete the form provided in Appendix 1 to these Terms and send it to support@tedee.com. Tedee will provide access to your Data in line with these Terms and applicable law, including the EU Data Act.
- 4.1.3. If your request concerns personal data and you are not the data subject, Tedee will share such data only if there is a valid legal basis under Article 6 of the GDPR, and, where applicable, the conditions of Article 9 of the GDPR and Article 5(3) of the ePrivacy Directive (Directive 2002/58/EC) are met.
- 4.1.4. In such cases, you must specify in your request the relevant legal basis under the GDPR (and, where applicable, the corresponding exception under Article 9 of the GDPR and Article 5(3) of the ePrivacy Directive) that justifies the sharing of personal data.
- 4.1.5. Tedee will make your Data available free of charge, with at least the same level of quality as it is available to Tedee. The Data will be provided in a comprehensive, structured, commonly used, and machine-readable format, together with any metadata needed to interpret and use it.
- 4.1.6. You and Tedee may use the services of a third party (including a Data Intermediation Services provider as defined in Article 2 of Regulation

(EU) 2022/868) to enable you to exercise your rights under this Section. Such a third party will not be considered a “Data Recipient” under the Data Act unless it processes the Data for its own business purposes. The party requesting the involvement of such a third party must notify the other party in advance.

4.1.7. The Data Recipient shall erase the Data once it is no longer necessary for the purpose defined by the User.

4.1.8. If you identify any issue or incident related to your Data or your access to it, please notify Tedee with a detailed description of the problem at support@tedee.com. You and Tedee will cooperate in good faith to identify the cause and resolve the issue as soon as reasonably possible. If Tedee is responsible for the incident, it will promptly take corrective actions to remedy it.

4.1.9. Tedee may restrict or suspend access to certain Data only where this is necessary to protect its legitimate business interests, trade secrets, the rights of third parties, or the security and integrity of its services. In such cases, Tedee will inform you of the reason for the restriction, unless providing such information would compromise the purpose of the restriction (for example, for security or fraud-prevention reasons).

5. Unilateral changes by the Data Holder

5.1. Tedee may, in good faith, make unilateral changes to the Data specifications or access arrangements described in Sections 2.1 and 2.2, if such changes are objectively justified by Tedee’s normal business operations — for example, due to a necessary technical modification, a newly identified security vulnerability, or an infrastructure update.

5.2. In such cases, Tedee will notify you of the change without undue delay after the decision is made.

5.3. If the change may significantly affect your ability to access or use the Data, Tedee will notify you in advance, within a reasonable period before the change takes effect.

5.4.A shorter notice period may apply only where advance notice is impossible or unreasonable in the circumstances, such as when immediate changes are required to fix a critical security issue.

6. Unauthorised use and sharing of data

You agree not to engage in any of the following:

- a) using the Data to develop or assist in developing a connected product or service that competes with Tedee Products, or sharing the Data with a third party for that purpose;
- b) using the Data to analyse or draw conclusions about Tedee's financial situation, business model, or production methods;
- c) using coercive means or exploiting vulnerabilities in Tedee's systems to obtain access to Data;
- d) sharing the Data with a third party designated as a gatekeeper under Article 3 of Regulation (EU) 2022/1925 (the Digital Markets Act);
- d) using the Data in any way that violates EU law or applicable national law.

7. Sharing your Data with third parties

7.1.You may ask Tedee to share your Data with a third party of your choice (a “**Data Recipient**”), for example another service provider or application you want to connect to your Tedee device.

7.2.You can submit such a request using the form available in Appendix 2 to these Terms and send it to support@tedee.com

7.3.Tedee will make your Data available to the Data Recipient free of charge for you, in a structured, commonly used, and machine-readable format, together with the necessary metadata so that it can be interpreted and used.

7.4.If the requested Data includes personal data of other persons, Tedee will only share it when there is a valid legal basis under the GDPR or other

applicable law.

7.5. Tedee may refuse or restrict sharing your Data only where this is necessary to protect its legitimate interests, trade secrets, the rights of others, or the security and integrity of its systems.

8. Limitations of your rights

8.1. Tedee may temporarily limit or suspend your right to use or share certain Data where required by law, to protect the security of the platform, or to prevent misuse of the Data.

8.2. In such cases, Tedee will notify you about the limitation and restore your access as soon as the issue is resolved.

9. Compensation

9.1. If Tedee restricts your rights to use or share your Data beyond what is permitted under these Terms or applicable law, you may be entitled to reasonable compensation in accordance with the Data Act.

9.2. If monetary compensation applies, statutory interest will accrue on any delayed payments in line with applicable law. Tedee remains entitled to request reasonable, non-discriminatory compensation provided you are not classified as small and medium-sized enterprises (SMEs), in line with Article 9 of the Data Act.

10. Transfer of product ownership or multiple users

10.1. If you sell, give away, or otherwise transfer your Tedee device to another person (“Subsequent User”), your rights and obligations under these Terms end once the new owner sets up their own Tedee account.

- 10.2. Please make sure to delete your personal Data from the device and remove your credentials before handing it over.
- 10.3. If you share the use of your device with others (“Additional Users”), each user must have their own Tedee account and will enter into a separate agreement with Tedee.
- 10.4. If a device can be used without a Tedee account, Tedee may not be able to identify the new user or ensure that Data from previous use is deleted. In such cases, you are responsible for ensuring that any new or shared users are properly informed and that your Data is removed or anonymised before the transfer.

11. Before transferring the Product:

- a) delete your account or remove your access credentials from the Product and Tedee App so that the Subsequent User cannot use your account;
 - b) inform Tedee of the transfer by contacting support@tedee.com
 - c) if the Product allows storage of Data locally, make sure any personal or sensitive information is erased before the transfer.
- 11.1. The new owner (Subsequent User) will need to create their own Tedee account to use the Product and related services. Once the new account is created, your rights and obligations under these Terms automatically end.
- 11.2. Tedee may continue to use or retain Data generated before the transfer if such use is necessary to perform its legal, contractual, or security obligations.

12. Shared use

- 12.1. If you allow another person to use your Product or related services (“**Additional User**”), you must ensure that each user has their own Tedee account and uses the Product in compliance with these Terms.
- 12.2. If an Additional User uses the Product without creating a separate Tedee account, you remain responsible for ensuring that they use the Product lawfully and do not access your personal Data.
- 12.3. If Tedee receives a request or claim from an Additional User relating to Data access or use, Tedee may contact you to help resolve the issue.

13. Responsibility for transfers

If you do not follow the above rules and Tedee continues processing Data linked to you after a transfer or shared use, you may be responsible for any resulting claims or damages caused to Tedee or other users.

14. Duration and termination of the contract

- 14.1. These Terms take effect when you create a Tedee account or activate your Tedee Product or related service, whichever occurs first.
- 14.2. The contract between you and Tedee remains in force for an indefinite period, unless it ends in one of the cases described below.

15. Termination

15.1. These Terms cease to be binding:

- a) when your Tedee Product is permanently deactivated, destroyed, or otherwise stops generating Data;
- b) when you sell, give away, or otherwise transfer ownership of your Tedee Product, or when your right to use the Product or related service ends (for example, at the end of a lease or subscription period); or
- c) when both you and Tedee agree to end the contract, including if it is replaced by a new one.

15.2. If a new owner (Subsequent User) or another person (Additional User) starts using the Product, the contract between you and Tedee ends, but a new contract will automatically be formed between Tedee and that new user when they activate or register the Product.

16. Effects of termination

16.1. Upon termination of these Terms:

- Tedee will cease collecting or generating Data from your Product or Related Service;
- Tedee may continue to store or process Data generated prior to termination to the extent required by applicable law, security standards, or contractual obligations, as specified in these Terms and in the Tedee Privacy Policy.

16.2. Termination does not affect any rights or obligations that accrued prior to its effective date. Provisions concerning confidentiality, applicable

law, dispute resolution, and other clauses which by their nature are intended to survive termination shall remain in full force and effect.

17. Remedies for breach of Terms

- 17.1. A breach of these Terms happens when either you or Tedee do not fulfil your contractual obligations in a way that significantly affects the other party or causes harm.
- 17.2. A failure to perform is not considered a breach if it results from circumstances outside the party's reasonable control (for example, a power outage, cyberattack, or system failure) and could not reasonably have been prevented. In such cases, the affected party must notify the other party as soon as possible.

18. Remedies available to you

- 18.1. If Tedee fails to meet its obligations under these Terms:
- a) you may ask Tedee to correct the issue or comply with its obligations without undue delay;
 - b) you may request that Tedee deletes Data that was accessed or used in violation of these Terms;
 - c) if Tedee's breach causes you actual financial damage, you may seek compensation in accordance with applicable law.
- 18.2. You may also temporarily withdraw Tedee's permission to use your Data (as described in these Terms) if Tedee fails to comply, unless doing

so would cause disproportionate harm to Tedee or the operation of the services.

19. Remedies available to Tedee

If you breach these Terms (for example, by using the Product unlawfully, manipulating technical protections, or violating Data security obligations):

- a) Tedee may suspend or limit your access to Data or services until you correct the issue;
- b) Tedee may request that you delete Data or content obtained or used in violation of these Terms;
- c) Tedee may seek compensation if it suffers losses caused by your intentional or grossly negligent conduct.

20. Confidentiality

20.1. Tedee and you agree to keep confidential any non-public information obtained in connection with the use of Tedee products, related services, or these Terms. This includes, in particular:

- a) technical or business information about Tedee's systems, products, or operations;
- b) information about you or other individuals, unless such information has been made public by the person concerned; and
- c) details of how this contract is performed, including any issues or disputes arising during its execution.

20.2. Both you and Tedee must take reasonable steps to protect such information and not share it with third parties unless:

- a) disclosure is required by law or by a competent authority;
- b) disclosure is necessary to perform these Terms (for example, to trusted service providers or partners under confidentiality obligations); or
- c) the other party has given prior consent.

20.3. These confidentiality obligations continue to apply even after this contract ends.

20.4. Nothing in this section limits or replaces Tedee's obligations under applicable data protection laws, including the GDPR, the ePrivacy Directive, and other relevant EU or national legislation.

21. Final provisions

21.1. This Contract is governed by the law of Poland.

21.2. These Terms (together with any appendices or other documents referred to in them) represent the entire agreement between you and Tedee regarding your use of Tedee Products, related services, and Data. They replace any previous versions or communications, whether written or oral, relating to the same subject matter.

21.3. Tedee may update or modify these Terms from time to time, for example to reflect changes in the law, technology, or how our services work. You will be notified of any significant changes in advance, for example by email or through the Tedee App. Continued use of your Tedee Product or services after the effective date of an update means that you accept the revised Terms.

21.4. If any provision of these Terms is found to be invalid, illegal, or unenforceable, the remaining provisions will continue to apply. Any gaps or

ambiguities will be interpreted in accordance with applicable law and the principle of good faith.

- 21.5. If any ambiguity cannot be resolved through these Terms, it will be interpreted according to the applicable law (as set out in the section on governing law) and in a fair and reasonable manner consistent with good faith and the objectives of the Data Act.
- 21.6. Tedee aims to resolve any issues or disputes with you in a fair and cooperative way. If a dispute arises, please first contact support@tedee.com, and Tedee will make every effort to resolve it amicably.
- 21.7. If the issue cannot be resolved directly, you may submit the dispute to an independent dispute settlement body in line with Article 10 of the Data Act, or file a complaint with the competent national authority designated under Article 37 of the Data Act. This does not affect your right to bring a claim before a competent court in your country of residence or any other court that has jurisdiction under applicable law.

Version history:

- Rev. 1.0. - October, 15, 2025

Appendix 1: Form for an access request by the User

Identification of the User	Name: <i>Specify</i> Contract n°: <i>Specify</i>
Identification of the person making the request on behalf of the User (if applicable)	Name: <i>Specify</i> Relationship with the User: <i>Specify</i>
Products and/or Services concerned by the request	Product/Service 1: <i>Specify (e.g. serial number)</i> Product/Service 2: <i>Specify (e.g. serial number)</i>
Data concerned by the request	☐ All data which is readily available to the Data Holder ☐ Including personal Data <i>If the User is not the data subject, specify valid legal basis for processing under Article C of Regulation (EU) 201C/C7S and, where relevant, how the conditions of Article S of that Regulation and of Article 5(3) of Directive 2002/58/EC are fulfilled</i> ☐ After anonymization

	☐ Only non-personal Data ☐ Other: <i>Specify</i>
Date of Data concerned by the request	☐ Past data: <i>Specify the period</i> ☐ Future data: <i>Specify the period</i>
Timing of access to the Data (<i>depending on what is agreed in clause 4.3.2</i>)	☐ Without undue delay ☐ Continuously ☐ Realtime ☐ With appropriate frequency ☐ Other: <i>please specify</i>
Modalities for access to the Data	☐ Option 1 proposed by Data Holder ☐ Option 2 proposed by Data Holder
Destination for the transfer:	<i>Specify depending on the answer to the previous point</i>
Date of the request	<i>Specify</i>

Appendix 2: Form for an access request by the User to make data available to a third party

Identification of the User	Name: <i>Specify</i> Contract n°: <i>Specify</i>
Identification of the person making the request on behalf of the User (if applicable)	Name: <i>Specify</i> Relationship with the User: <i>Specify</i>
Products and/or Services concerned by the request	Product/Service 1: <i>Specify</i> Product/Service 2: <i>Specify</i>
Data concerned by the request Please note: does not apply in the context of the testing of new connected products, substances or processes that are not yet placed on the market	All data which is readily available to the Data Holder
If the data includes personal data	<i>Specify valid legal basis for processing under Article 6 of Regulation (EU) 2016/679 and, where relevant, how the conditions of Article 9 of that Regulation and of Article 5(3) of Directive 2002/58/EC are fulfilled</i>
Identification of the third party Please note: cannot be a gatekeeper under Article 3 of Regulation (EU) 2022/1925	Name: <i>Specify</i> Contact details: <i>Specify</i>