PRIVACY POLICY

Last Updated: 21st April 2022

BaseUp Technologies Inc. and our affiliated company BaseUp Technologies Pty Ltd. (collectively "**BaseUp**," **Company**," "**us**," "**our**," or "**we**") respect your privacy and we are committed to protecting it through our compliance with this Privacy Policy.

Scope

This Privacy Policy describes and applies to the types of information we may collect from you or that you may provide when you visit the website https://www.baseup.com (our "**Website**"), or contact us directly offline, or we may collect about you when you inquire about using or use our Services (defined below), and our practices for collecting, processing, using, maintaining, protecting, and disclosing such information.

"**Services**," as used herein, are defined as the administrative, technical, and physical functionality related to our: (i) **dashboard** (service provided via contract with our Customers), (ii) **driver app** (service provided to Drivers based on contract with our Customers); and (ii) **access control platform** (service provided via contract with our Customers). A "**Customer**," as used herein, is defined as an individual or company that uses one or more of our Services. A "**Driver**," as used herein, is defined as a person authorized to access and use our driver app to access parking spaces.
PLEASE READ THIS PRIVACY POLICY CAREFULY TO UNDERSTAND OUR POLICIES AND PRACTICES REGARDING YOUR INFORMATION AND HOW WE WILL TREAT IT. IF YOU DO NOT AGREE WITH OUR POLICIES AND PRACTICES, YOUR CHOICE IS NOT TO USE OUR WEBSITE OR SERVICES. BY ACCESSING OR USING OUR WEBSITE OR SERVICES, YOU AGREE TO THIS PRIVACY POLICY. THIS POLICY MAY CHANGE FROM TIME TO TIME. YOUR CONTINUED USE OF OUR WEBSITE OR SERVICES AFTER WE MAKE CHANGES IS DEEMED TO BE ACCEPTANCE OF THOSE CHANGES, SO PLEASE CHECK THIS POLICY PERIODICALLY FOR UPDATES.

This Policy does not apply to information we collect/process on behalf of our Customers as a service provider or data processor. Such processing is governed by our Customer contracts and if you have query as to how our Customers use your information you should address it directly to them. This Policy does, however, apply to certain information processing for the purpose of improving our Services.

California residents may have additional rights and choices. To learn more about your California privacy rights, please see our **Privacy notice for California residents** below.

Information we collect

We collect/process several types of information from and about users of our Website and/or Services, including: (i) "**Personal Data**," which the EU General Data Protection Regulation 2016/1679 (GDPR) defines as any information relating to an identified or identifiable data subject; (ii) "**Personal Information**," which the California Consumer Privacy Act of 2018 (CCPA) defines as information that directly or indirectly identifies, relates to, describes, is reasonably capable of being associated with, or can reasonably be linked to a particular consumer or household, (iii) information or data that is about you, but in a form that does not, on its own, permit direct association with you (e.g., sex, age, language preference, occupation, or the like); and (iv) information or data about your interaction with (or use of) our Website or Services, which may include your Internet connection, the equipment you use to access our Website or Services, and details relating to your use of our Website or Services.

Information we collect directly from you

We collect/process information received directly from you when you provide it to us, which may include information you provide to us: (i) through e-mail, messages, chat rooms, surveys, blogs, or our Website or Services; (ii) offline when you contact us in writing or by telephone, including when you contact customer support; (iii) at the time of registering and/or subscribing to use our Website or Services; or (iv) when you report a problem with our Website or Services, including when you contact our technical support. This information may include your name, contact information, license plate number. ("**Client Data**")

Different forms on our Website (e.g., registration form) may also collect your name, e-mail, phone number, company name (if applicable), country, area, zip code, address, password or other data to help you with your experience. Provision of such contact information is voluntary, unless the relevant forms specify that this data is necessary for use of our Website and/or the Services.

When using our Services, you may be required to provide billing information. This information is required by us to verify your identity, and invoice you (if applicable).

For the purposes of European data protection laws, we process information collected directly from you on the basis of our legitimate interests, that are to deliver, manage, improve and promote our Services to our Customers and prospective Customers.

Information we collect through automatic data collection technologies

In addition to any information that we collect/process directly from you, we may use a variety of technologies that automatically (or passively) collect/process certain information or data whenever you visit or interact with our Website or while using our Services.

We do not treat information collected by automatic data collection technologies as Personal Data or Personal Information. However, to the extent that Internet Protocol (IP) addresses, or similar identifiers are considered Personal Data or Personal Information by a relevant law or regulation, we will also treat these identifiers as Personal Data or Personal Information. Similarly, to the extent that information or data we collect/process that is not considered Personal Data or Personal Information is combined with Personal Data or Personal Information, we treat the combined information as Personal Data or Personal Information for the purposes of this Privacy Policy and compliance with relevant laws and regulations.

The technologies we use for automatic data collection may include:

Cookies. A cookie is a small file placed on the hard drive of your computer. You may set your browser to notify you or decline the receipt of Cookies. Please note that such settings do not prevent the collection or processing of Personal Data or Personal Information about you, as otherwise provided herein. Moreover, certain features of our Website may not function properly or be available if your browser is configured to disable cookies and/or other automatic data collection technologies.

The following "cookies" are automatically downloaded on any device used to access our Website and/or one or more of our Services:

Cookie Name	Purpose	Category
_legacy_auth0.is.authenticated auth0.is.authenticated ajs_group_id ajs_user_id ajs_anonymous_id	We use these cookies to authenticate user access to our driver app and dashboard.	Strictly Necessary

Please exercise your choice with respect to accepting or rejecting "cookies" via the pop-up on our Website (the shield icon). In addition, you can block these cookies and similar technologies by changing your browser setting. Please note, however, that such settings do not prevent the collection or processing of Personal Information or Personal Data about you, as otherwise provided in this Privacy Policy. Moreover, certain features of our Website, Application(s) or Services may not function properly or be available if your browser is configured to disable Cookies and/or any of the other automatic data collection technologies discussed above.

Information or data obtained by us with the use of automatic data collection technologies may include:

- Internet Protocol (IP) addresses;

- Device or mobile IDs and/or device model and type;
- Browser information, operating system information, and/or language preferences;
- The location and the preceding and succeeding websites you have visited, including which pages/part/icons on the Website you interacted with;
- Applications you click on and how often; and
- The pages of our Website you visit, and how long you spend on each page.

For the purposes of data protection law, we use the following justifications for our use of information or data obtained with the use of automatic data collection technologies:

Automatic or passive collection technologies help us better understand user behavior, tell us which parts of our Website you have visited, stayed on, and facilitate and measure the effectiveness of advertisements and web searches. These technologies can also be used to help us understand your preferences based on previous or current Website activity, which enables us to provide you with improved Services. We also use these technologies to help us compile aggregate data about our Website traffic and interaction with the Website so that we can offer you better experience and tools in the future.

How we may use information we collect

In addition to uses described above, we may use information that you provide to us, we collect about you or that we obtain from our Customers, including any Personal Information or Personal Data:

- To present our Website and its contents to you.
- To provide you with information, products, or services that you request from us.
- To fulfill any other purpose for which you provide it.
- To provide you with notices about your account/subscription, including expiration and renewal notices.
- To carry out our obligations and enforce our rights arising from any contracts entered into between you and us, including for billing and collection.
- To notify you about changes to our Website or any products or services we offer or provide though it.
- To allow you to participate in interactive features on our Website.
- To personalize and develop our Website, products, and services and to understand user behavior.
- For testing, research, analysis, and product development, including to develop and improve our Website and Services in order to better serve you and/or to provide Services more effectively.
- To process and request payments involving your account.
- To help BaseUp compile aggregate data about our Website traffic and interaction with the Website or Services so we can offer you a better experience and tools in the future.
- In any other way we may describe when you provide the information.
- For any other purpose with your consent.

Disclosure of information we collect

We may use a third party (e.g., processor, sub-processor, service provider, contractor, partner or supplier, vendor, etc.) to perform certain business-related functions. Examples of such functions include, but are not limited to: data storage services, analytics, debugging, technical resolution, product improvement, database maintenance services, mailing, and payment processing. When we use a third party to perform services on our behalf, we will only provide them with access to Personal Information or Personal Data that they need to perform their specific function. We will make sure that each third party will be required by contract to keep such Personal Information or Personal Data confidential, make necessary steps to protect such Personal Information or Personal Data, and not to use it for any purpose other than providing services to us and other provisions as required by law or regulation.

We use the following service providers/processors:

Service	Service Provider/ Processor	Purpose	Link to Service Provider/Processor Privacy Policy
Google Inc.	Google Inc.	Cloud infrastructure	https://cloud.google.com/terms/cloud-privacy-notice
Auth0 Inc.	Auth0 Inc.	Authentication	https://auth0.com/privacy
Stripe	Stripe	Payment processing	https://stripe.com/privacy
Zendesk	Zendesk	Customer support software	https://www.zendesk.com/company/agreements-and-terms/privacy-policy/
Postmark	Postmark	E-mail delivery services	https://wildbit.com/privacy-policy
Datadog	Datadog	Error tracking and observability	https://www.datadoghq.com/legal/privacy/
Twilio	Twilio	SMS delivery service	https://www.twilio.com/legal/privacy

Before transferring any Personal Data or Personal Information to a third party (processor, service provider, contractor, affiliate, partner, contractor, supplier, vendor etc.) we shall make reasonable checks of such third party regarding its compliance with the applicable laws.

Compliance with laws and law enforcement entities

We may disclose Personal Information or Personal Data if required to do so by law or to comply with a legal obligation, or if we believe in good faith that such action is necessary to: (i) protect our rights or property and our customers, or (ii) protect the property or safety of users of our Website or Services or any third party. If we will be required by law to disclose any of your Personal Information or Personal Data, we will use reasonable efforts to provide you with notice

of that disclosure requirement, unless we are prohibited from doing so by statute, court or administrative order.

Business transfers

We reserve the right to sell, assign, or transfer our business or assets. In any such event or similar event, including but not limiting to a corporate sale, merger, reorganization, dissolution, etc., Personal Information or Personal Data may be part of the transferred assets. You acknowledge that such transfers may occur and that any acquirer or successor of ours may continue to use your Personal Information or Personal Data as set forth in this Privacy Policy.

Your rights

Under European data protection law, you have various rights in relation to your Personal Data. All of these rights can be exercised by contacting us at privacy@baseup.com.

In certain circumstances, you have the right to:

- be informed (or the processing);
- access (such information);
- rectification (of inaccurate information);
- erasure (of such information);
- restrict processing (in certain cases);
- object to profiling;
- data portability (in certain cases);
- complain to the Information Commissioner's Office; and
- withdraw consent (if we have collected your Personal Information/Data on this basis).

Detailed information on the full content of your rights (and any conditions that may apply) is provided by the United Kingdom's Information Commissioner's Office and is available on their website: https://ico.org.uk/your-data-matters.

California residents may have additional rights and choices regarding the disclosure of information we collect. To learn more about your California privacy rights, please our **Privacy notice for California residents** section below.

Asking us to stop processing your Personal Data or Personal Information or deleting your Personal Data or Personal Information will likely mean that you will no longer be able to use our Services, or at least those aspects of the Services that require the processing of the types of Personal Data or Personal Information you have asked us to delete.

Where you request BaseUp to rectify or erase your Personal Data or Personal Information or restrict any processing of such Personal Data or Personal Information, BaseUp may notify third

parties to whom such data/information has been disclosed of such request. Such third party may, however, have the right to retain and continue to process such Personal Data or Personal Information in its own rights.

While we will not sell your Personal Information or Personal Data (or any other data you provide us) to third parties, we reserve the right to share any data that has been anonymized. You acknowledge and accept that we own all right, title and interest in and to any derived data or aggregated and/or anonymized data collected or created by us.

How long we retain your Personal Data/Information

We may retain the above information for as long as is required to fulfill the purposes of the processing of the Personal Data or Personal Information as outlined in this Privacy Policy, or for a longer period as required according to the applicable law. Retention period will be determined taking into account the type of information that is collected and the purpose for which it is collected, bearing in mind the requirements applicable to the situation and the need to destroy outdated, unused information at the earliest reasonable time.

If information is used for two purposes, we will retain it until the purpose with the latest period expires.

We restrict access to your Personal Information or Data to those persons who need to use it for the relevant purpose(s). Our retention periods are based on business needs and your information that is no longer needed is either irreversible anonymized (and the anonymized information may be retained) or securely destroyed. To determine the appropriate retention period for personal data/information, we consider the amount, nature, and sensitivity of the Personal Data/Information, the personal risk or harm from unauthorized use or disclosure, the purpose for which we process your Personal Data or Personal Information and whether we can achieve those purposes through other means, and applicable legal requirements.

How we protect your Personal Data/Information

BaseUp is committed to achieving and maintaining the trust of users of our Website and our Customers. Integral to this mission is providing a robust security and privacy program that carefully considers data protection matters related to the user of our Website and Services, and Customer Data.

No data transmission over the internet or website can be guaranteed to be secure from intrusion. However, we maintain commercially reasonably physical, electronic and procedural safeguards to protect your Personal Data and Personal Information in accordance with data protection legislative requirements.

Sensitive information between your browser and our Website is transferred in encrypted form using secure socket layer (“SSL”) or equivalent cryptographic protocols using certificates issued by a trusted third-party authority.

Control of processing

BaseUp has implemented procedures designed to ensure that Client Data is processed only as instructed by BaseUp, throughout the entire chain of processing activities by BaseUp processors/service providers. In particular, BaseUp has entered into written agreements with certain sub-processors/service providers containing privacy, data protection, and data security obligations that provide a level of protection appropriate to their processing activities. Compliance with such obligations as well as the technical and organizational data security measures implemented by BaseUp processors/service providers are subject to regular audits.

Security controls

Our Services include a variety of security controls. These controls include:

- Role concepts with differentiated access rights on the basis of identity management and secure authentication methods are in place.
- Validation controls are in place to filter out inconsistent, incomplete and inaccurate data.
- Retention schedules and deletion triggers have been set and data inventory review and deletion processes are in place.
- Unique user identifiers allow customers to assign unique credentials for their users and assign and manage associated permissions and entitlements.
- Passwordless login to prevent user password storage.
- Single Sign On (SSO) to prevent federated authentication.
- s.

Security policies and procedures

Our Services are operated in accordance with the following policies and procedures to enhance security:

- Regular software updates for the Services, logical access controls, data backups and network authentication are used.
- Internal security awareness and training at BaseUp.
- User access log entries will be maintained, containing date, time, User ID, URL executed, or identity ID operated on, operation performed (accessed, created, edited, deleted, etc.) and source IP address.
- If there is suspicion of inappropriate access to the Services, BaseUp can provide customers log entry records to assist in forensic analysis. This service will be provided to customers on a time and materials basis.
- User access logs will be stored in a secure centralized host to prevent tampering.
- BaseUp personnel will not set a defined password for a user.

Intrusion Detection. BaseUp, or an authorized independent third party will monitor the Services for unauthorized intrusions using network-based intrusion detection mechanisms. BaseUp may analyze data collected by users' web browsers (e.g., device type, screen resolution, time zone, operating system version, browser type and version, system fonts, installed browser plugins, enabled MIME types, etc.) for security purposes, including to prevent fraudulent authentications, and to ensure that the Services function properly.

Security Logs. All BaseUp systems used in the provision of the Services, including firewalls, routers, network switches and operating systems, log information to their respective system log facility or a centralized syslog server (for network systems) in order to enable security reviews and analysis.

Incident Management. BaseUp maintains security incident management policies and procedures. BaseUp notifies impacted customers without undue delay of any unauthorized disclosure of their respective Customer Data by BaseUp or its agents of which BaseUp becomes aware to the extent permitted by law.

User Authentication. Access to our Services requires a valid user ID and password combination, which are encrypted while in transmission, as well as machine specific information for identity validation as described under "Security Controls," above. Following a successful authentication, a random session ID is generated and stored in the user's browser to preserve and track session state.

Physical Security. Production data centers used to provide the Services have access control systems. These systems permit only authorized personnel to have access to secure areas. These facilities are designed to withstand adverse weather and other reasonably predictable natural conditions, are secured by around- the-clock guards, two-factor access screening, including biometrics, and escort-controlled access, and are also supported by on-site back-up generators in the event of a power failure.

Reliability and Backup. All infrastructure components are configured in a high availability mode or in a redundant fashion. All Customer Data submitted to the Services is stored on infrastructure that supports high availability and is backed up on a regular basis. This backup data is retained for thirty (30) days.

Disaster Recovery. The Services' production systems are protected by disaster recovery plans which provide for backup of critical data and services. A comprehensive system of recovery processes exists to bring business-critical systems back online within the briefest possible period of time. Recovery processes for database security, systems administration, and network configuration and data provide a roadmap for personnel to make processes available after an outage.

Data Encryption. The Services use, or enable Customers to use, industry-accepted encryption products to protect Customer Data and communications during transmissions between a customer's network and the Services including through Transport Layer Encryption (TLS) leveraging at least 2048-bit RSA server certificates and one-hundred-twenty-eight (128) bit symmetric encryption keys at a minimum.

Data Anonymization. BaseUp anonymizes/de-identifies Customer Data ("**Anonymized Data**") prior to storing the data such that no personally identifiable information is contained in the Anonymized Data, nor any data that would identify Customers, their users, Customers' clients, or any individual, company or organization. BaseUp combines the Anonymized Data to improve its algorithms to provide increasing benefits to customers. We also refer to this as "**Aggregate Data**".

Exports outside the US

Your personal information may be accessed by our staff or suppliers in, transferred to, and/or stored at, a destination outside the United States (US) in which data protection law may be of a lower standard that in the US. Regardless of location or whether the person is an employee or contractor, we will impose the same data protection safeguards that we deploy inside the US.

Exports outside the EEA or UK

Your personal information may be accessed by staff or suppliers in, transferred to, and/or stored at, a destination outside the European Economic Area (EEA) or the United Kingdom (UK) in which data protection law may be of a lower standard that in the EEA or the UK. Regardless of location or whether the person is an employee or contractor, we will impose the same data protection safeguards that we deploy inside the EEA or UK.

Certain countries outside the EEA and the UK have been approved by the European Commission and the Information Commissioner's Office as providing essentially equivalent protections to EEA and UK data protection laws and therefore no additional safeguards are required to export Personal Data to these jurisdictions. In countries that have not had these approvals, we will transfer it subject to the European Commission and Information Commissioner's Office approved contractual terms that impose equivalent data protection obligations directly on recipient, unless we are permitted under applicable data protection law to make such transfers without such formalities.

Please contact us at privacy@baseup.com if you would like further details of the specific safeguards applied to the export of your Personal Data.

Privacy notice for California residents

If you are a consumer located in California, we process your Personal Information in accordance with the California Consumer Privacy Act (CCPA). This section provides additional details about the Personal Information we collect and use for purposes of CCPA.

The Information we collect, Information we collect directly from you, and **Information we collect through automatic data collection technologies** sections above describe the Personal Information we may have collected about you within the last twelve (12) months, including the categories of sources of that information. We collect this information for the purposes described in the **How we may use information we collect** section. We disclose this information as described in the **Disclosure of information we collect** section.

Your CCPA Rights and Choices. As a California consumer and subject to certain limitations under the CCPA, you have choices regarding our use and disclosure of your Personal Information:

- **Exercising the right to know**: You may request the following information about the Personal Information we have collected about you (see above under Your Rights):

    - the categories and specific pieces of Personal Information we have collected about you;
    - the categories of sources from which we collected the Personal Information;
    - the business or commercial purpose for which we collected the Personal Information;
    - the categories of third parties with whom we shared the Personal Information; and
    - the categories of Personal Information about you that we disclosed for a business purpose, and the categories of third parties to whom we disclosed that information for a business purpose.

- **Exercising the right to delete**: You may request that we delete the Personal Information we have collected from you, subject to certain limitations under applicable law.

- **Exercising the right to opt-out from a sale**: You may request to opt out of any "sale" of your Personal Information that may take place. We do not use, share, rent or sell the Personal Information of our customers for interest-based advertising. We do not sell or rent the Personal Information of our customers or our site visitors.

- **Non-discrimination**: The CCPA provides that you may not be discriminated against for exercising these rights.

Children under age 18

Our Website and Services are not intended for children under eighteen (18) years of age (or age equivalent in the relevant jurisdiction). No one under the age of eighteen (18) may provide any information to or on our Website, and/or Services. We do not knowingly collect Personal Data or Personal Information from children under eighteen (18). If you are under eighteen (18), do not use or provide any information to or on our Website or Services, make any purchases through our Website or Services, use any of the interactive or public comment features of this Website or provide any information about yourself to us, including your name, address, telephone number,

e-mail address, or any screen name or username you may use. If we learn that we have collected or received Personal Data or Personal Information from a child under eighteen (18) without verification of parental consent, we will delete that information. If you believe we might have any information from or about a child under 18, please e-mail us at privacy@baseup.com.

Direct marketing

From time-to-time we may use your personal information to provide you with information about our services, changes to our organization, or new products or services being offered by us.

By accepting BaseUp's terms and conditions and the terms of this Privacy Policy and by providing BaseUp with information or seeking its Services, you consent to receiving direct marketing of relevant services or opportunities by BaseUp.

If you do not wish to receive marketing information, you may at any time opt out or decline to receive marketing information by contacting us at team@baseup.com or using the methods detailed in the "**Contact Information**" paragraph below. If the direct marketing is by email you may also use the unsubscribe function. We will not charge you for giving effect to your request and will take all reasonable steps to meet your request at the earliest possible opportunity.

Personal Information about other people

You must not provide personal information to BaseUp about another person, unless that person has authorized us, through you, to collect, use and disclose personal information about that person for the purposes described in this Privacy Policy.

Changes to our privacy policy

It is our policy to post any changes we make to our Privacy Policy on this page. If we make material changes to how we treat our users' Personal Information or Personal Data, we will notify you through a notice on our Website home page. The date the Privacy Policy was last revised is identified at the top of the page. You are responsible for periodically visiting our Website and this Privacy Policy to check for any changes.

No rights of third parties

The Privacy Policy does not create rights enforceable by third parties.

Contact information

If you have any questions, concerns or complaints regarding this Privacy Policy, or regarding a contact person (representative) for compliance with the relevant law or regulation, you can reach us at: privacy@baseup.com.