

Content

1. Introduction
2. General Terms and Conditions
3. Support Terms
4. Privacy Policy - User
5. Data Security Standards

Introduction

The terms and conditions herein, each specified under Content above are collectively referred to as **Contractual Terms and Policies** and apply to Accessy AB's (**Accessy**) operated Access control services and application (the **Service**). The terms and conditions herein shall, unless stated otherwise, apply in the order they are presented under Content above. This order shall also apply in the event of conflicting terms.

By downloading Accessy's App and subscribing to the Service, you will be a **User** and you agree to be bound by these Contractual Terms and Policies.

If you have questions or complaints regarding the Contractual Terms and Policies or about the Service, or otherwise about Accessy, please write to us at support@accessy.se.

General Terms and Conditions

1. Definitions

A-beamer - A physical badge, sticker or unit configured for the Service and mounted at each Device. A Member scans the A-beamer with a mobile phone, identifies a Device and processes an Access. The A-beamer contains the actual command to be executed, more explicitly, to open the door lock.

Access - Access to an Asset. A Member may have one or multiple Accesses and be granted Access by one or multiple Organizations. An Access is, for example, a User's/Member's permission to unlock a door.

Accessy - ACCESSY AB, a Swedish company having its main office at Södra Förstadsgatan 2, 211 43 Malmö, Sweden, registration number 559175-7082, acting both on its own name and on behalf of all legal entities within the Accessy Group.

Accessy Data - Data and materials supplied or made available by Accessy and/or its licensors to Users, Organization and its Administrators during the provisioning and support of the Service, Additional Services and App.

Accessy's Content - Any by Accessy and/or its licensors supplied texts, audio, video, graphics and other information and data as part of the provisioning and the support of the Service, Associated Services and Control Unit, App, and/or as published on Accessy's [website](#).

Accessy Group - Accessy and all subsidiaries or holding companies of Accessy including the ultimate holding company of Accessy and any subsidiary of that holding company from time to time.

Accessy's Technology - The Service, App, API, A-beamer, Control Unit and all Accessy's and/or its licensors technology (including but not limited to software, software development kits, hardware, products, processes, algorithms, user interfaces, know-how, techniques, designs and other tangible or intangible technical material or information), owned by Accessy and/or its licensors, and/or used in the course of providing and supporting the Service, App, API, A-beamer and subsequent updates or upgrades of any of the foregoing.

Administrator - Each Organization must appoint a User to be the administrator of a Subscription. The Organization can appoint one or several Administrators under the same subscription. The Administrator is, by appointment, authorized

by the Organization to connect and manage Assets and to invite Members to the Organization.

API - Application Programming Interface operated by Accessy (or its licensors) that permits the User to access certain functionality in the Service, and that enables the integration of the Service with other applications.

App - Accessy's software application that is necessary to control, utilize and interact with the Service. Accessy's App is available at [AppStore](#) (iOS) or [GooglePlay](#) (Android).

Applicable Data Protection Law - Refers to all privacy and personal data legislation applicable to the personal data including EU General Data Protection Regulation 2016/679 and any national laws adopted pertaining to this regulation. The term includes binding guidelines, opinions, recommendations and decisions from supervisory authorities, courts, or other authority (GDPR).

Asset - An object (usually a space) with an accompanying description, which includes one or several Devices. An Asset can be delegated, shares and granted Access to.

Customer- Each person or company completing the required registration process for Customer Agreement.

Customer Agreement – Agreement between Accessy and Customer for the paid subscription of the Service for the connection and administration of Assets, and for creating Organizations.

Device – A digital representation of the physical device that is connected to the Service (most often door-locks) and that belongs to a Subscription.

Documentation - Any Accessy and/or its licensors supplied specification, installation and security instruction, guide, manual and other documentation that explain the installation (if applicable), use and functions of the Service and Associated Services, including but not limited to related system and service documentation, all comments, procedural language, materials useful for understanding and using the Service and Associated Services.

Effective Date - The date when the User has completed the required registration process and subscription for use of the Service, including the setting up of the User Account.

General Terms - These General Terms and Conditions for Service.

Intellectual property rights or **IPR** - Patents, inventions, copyrights, trademarks, domain names, trade secrets, know-how and any other intellectual property and/or proprietary rights.

Member - A User that has become a member of an Organization. The Administrator of each Organization may invite a User (or approve a User's request) to become a Member of the Organization and to grant Access to connected Assets. When a User has become Member of an Organization the User is also granted access to that Organization's connected Assets, enabling the User to gain Access to such Asset. When becoming a Member, the Organization will keep records to identify the User as its Member.

Member Data - Data provided by a User to an Organization when the User is becoming a Member of the Organization (membership data), and any Transaction Data processed and created in or by the Service in connection with the User's use of the Organization's connected Assets. The Member identification is the User's first and last name in the User Account.

Organization - An organization is a specific identification (name), related to each Subscription. Each such identification is treated as a virtual organization in the Service.

Organization Data - connected Assets and Asset delegations, Member authorizations, permissions and user roles submitted to and stored in the Service by the Organization and its Administrators.

Personal Data - Any information relating to an identified or identifiable natural person (data subject), including User Account Data, where an identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as name, an identification number, location data, and online identifier.

Recovery Code - A User's own and unique code. The Recovery Code is provided to each User when registering for User Account and downloading the App. The Recovery Code is downloaded and stored as further detailed in Section 7. The Recovery Code is used by the User if the User does not have the Pin Code or has used the incorrect Pin Code leading to that the App will be in lock-mode. The Recovery Code is used to unlock the User Account and the App. If the User does not have a Recovery Code, the User will have to reset the User Account with the result of loss of Member Data.

Service - Accessy's software-as-a-service (SaaS) and cloud based operated access control services and products

ordered and subscribed by an Organization, and any subsequent updates, upgrades, and other services and/or products delivered or made accessible in connection with the Service. The Service does not include any Third-Party Services and Materials. The Service is made available online by Accessy, via the applicable login, the App and otherwise as designated by Accessy.

Service Data - Data provided to or generated by and in the Service, including Transaction Data.

Subscription - A Subscription of the Service is required to manage an Organization.

Support - Standard offsite support service provided by Accessy in accordance with the Accessy's [Support Terms](#).

Third-Party Services and Materials - Any third-party software, service, or product that is not provided by Accessy as part of the Service and that may be used by the Organization, its Administrator and Users in connection with or via the Service, for example, service subscriptions, external applications, access control systems, connectivity, mobile network services (mobile subscriptions), gateways, links, functionality, websites or materials and third-party content and data.

Transaction Data - Access transaction data (performed Accesses) generated by and in the Service, which include information of User's use of the Service and App.

User - The App and Service is intended for use by persons (each a User). To become a User a person must first install the App and complete the registration for an individual User Account in the Service.

User Account Data - The Users data provided by Users to Accessy for the registration of an individual User Service and App account with Accessy (**User Account**) for which the User is required to supply Accessy with User's first name, last name, and mobile telephone number. Membership in an Organization is linked to the User-profile in the User Account, and the User is identified by the User's mobile number, first and last name recorded in the User Account.

2. Scope of Terms and Service

These General Terms apply to Accessy and each User regarding the provision and use of the Service, App, and Support.

The User may subscribe for and use the Service and the App, by the User completing the required registration process for use of the Service and the App, and actively agreeing to be bound by these General Terms and attached exhibits, and any amendments and supplements thereto).

Nothing in these General Terms grants any ownership rights in Accessy's proprietary or intellectual property rights.

3. Changes to the General Terms

Accessy reserves the right to at any time change these General Terms to make them compliant with changes in legislation, decision of authorities on new or changed legislation or practises of courts, which in any way affect the provision of the Service, the App, or these General Terms.

4. Service and App license

Accessy and its licensors reserves all rights to the Service, the App, and Support not expressly granted herein.

Accessy grants to the User a non-exclusive, non-transferable, non-sub-licensable, and free of charge license to access and use the Service and the App.

The User acknowledges and agrees that the Service, is licensed and subscribed on a Software-as-a-service and/or cloud basis, and in no way sold or transferred.

The use of the Service and the App is personal. The User shall in no way sell, resell, rent, assign, share, outsource, included in network, or in SaaS-services or in external cloud computing environments or lend the Service and the App.

The User is only permitted to use the Service and the App unchanged 'as supplied by Accessy' and may not modify, decompile, reverse engineer, disassemble or otherwise attempt to derive and/or gain access to source code from any software made available as part of the Service, and the App (except where the foregoing is expressly prohibited by law, and then only to the extent so prohibited).

Accessy may, without prior notification to the User, make changes to the Service, the App or the method of providing them.

Access to and use of the Service and the App requires appropriate connections to the Internet and functional mobile

devices. The User is solely responsible for acquiring, installing, maintaining, and updating all hardware, mobile devices, computer software, and communications capability necessary for connecting to the Internet and for the use of the Service, and the App.

The User shall neither use nor permit others to use the Service, and the App for any unlawful, invasive, infringing, defamatory, fraudulent, or obscene purpose, or to alter, steal, corrupt, disable, destroy, trespass, or violate any security or encryption of any computer file, database, website, or network. User Accounts in the Service registered by 'bots' or other automated methods are prohibited.

Accessy is not responsible for the User's use of the Service, and the App, or for any other person acting on behalf of the User. The User is responsible for all activities that occur during use of the Service and the App. The User agrees to immediately notify Accessy of any unauthorized use of any Service and the App, or any other known or suspected breach of security.

5. Ownership

Accessy and its licensors, retain all rights, title, and interest in and to the Service, Associated Services, Accessy's Technology, Accessy Data, Accessy Content and Documentation and Accessy IPR. These rights are protected by the copyright laws and international copyright treaties.

Accessy retains all right, title, and interest, including without limitation all IPR to the Service and the App, App, API, software development kits, Accessy Technology, Documentation, Accessy's Content, Accessy Data and all updates, upgrades, modifications, enhancements, Accessy's Confidential Information, and other works deriving from the foregoing. No right, title or interest is granted, express or implied, to the User hereunder to any of the foregoing. The User agrees not, at any time, contest or aid others in contesting or doing anything which impairs the rights, title, or interest in or validity of any of any of Accessy's proprietary or intellectual property rights.

Accessy is granted the right (license) to access, display and use Your User Account Data and Transaction Data for as long as Your User Account is active or as needed to perform Accessy's obligations to You. Accessy's right includes the right to have Accessy's sub-contractors (including sub-processors) to use User Account Data and Transaction Data. Accessy also owns the right to use Your User Account Data and Transaction Data thereafter, in aggregate form and without any distinction special information about You, such use to be in accordance with Privacy Policy - User.

Accessy's right to use the User Account Data and Transaction Data also includes the collection and processing for the following purposes;

- (a) to ensure the security of the Services and other Accessy products, to detect and prevent use of the Service that is in violation of law or the terms and conditions for the Service,
- (b) to prevent abuse of the Service and User Accounts, and to detect and prevent fraud, etc, to ensure adequate and correct communication with the User in relation to the User Accounts,
- (c) to ensure adequate and correct communication with the User in relation to the User Account. Communication calls, emails, and support with Accessy's customer support may be recorded, analysed, and stored to train our employees and improve our ways of working, and
- (d) processing of different types of data to market our products and services, and for this purpose, Accessy may also compile statistics for analysis.

6. Access to Service and App

The Service and the App are provided by Accessy, via Accessy's operated system (including designated marketplaces for the App). The User shall access and use the Service the App, Accessy's portal or API, and/or Accessy's instructions. Access to and use of the Service and the App require appropriate Third-Party Services and Materials, in particular connections to mobile network services, and/or connections to the Internet or other relevant public electronic network.

Accessy is not liable to the User or to anyone else acting on behalf of the User for failure to maintain the confidentiality of their credentials for the Service, User Account and the App, and the User agrees to indemnify and hold Accessy harmless for any claims arising from loss of passwords.

7. Recovery Code

The Recovery Code is provided to each User when registering for User Account and downloading the App. The

Recovery Code is automatically stored in the Device's secure memory; if iCloud or Google Drive is used the Recovery Code will also be securely stored there. The User may at any time delete (or re-store) the Recovery Code at iCloud or Google Drive by using the App.

The Recovery Code may be used by the User if the User does not have the individual Pin Code or has used the incorrect Pin Code leading to that the App will be in lock-mode. The Recovery Code is used, at the User's option, to unlock the User's User Account or App. If the User does not have a Recovery Code the User will have to reset the User Account with the result of loss of Member Data (memberships and Accesses, including pending invitations).

The storage and management of the Recovery Code at iCloud and Google Drive are Third-Party Service (as governed herein) is not under the control of Accessy, and Accessy is not responsible for such services provided by iCloud and Google Drive, or any data storage and/or retrievals, changes, or updates to such services. Each provider of these Third-Party Service is responsible for storage, management, security, and such data, through its services and operating systems.

8. Support

Accessy's Standard offsite support service for the installation and use of the Service and the App will be provided by Accessy in accordance with the Accessy's [Support Terms](#).

9. Compliance

The User is not permitted to use, resell, distribute, transfer, provide, sub-license, share with, or otherwise offer the Service and the App in violation of any laws, and anti-corruption statutes in all jurisdictions. Without limiting the foregoing, the User is prohibited to re-export, transfer, make available or release (together **Export**) the Service and/or the App to any destination, person, entity, or other user prohibited or restricted under trade laws of related countries pertaining to the Export, import, use, or distribution of the Service and the App.

10. Personal Data

To the extent Accessy processes Personal Data Accessy shall treat such Personal Data in accordance with the terms and conditions set forth in [Accessy Privacy Policy](#).

11. Biometric data

The Service and Accessy do not take part in any collection, processing, or storage of any of biometric data, such as Face-ID, fingerprint, voice recognition. Each provider of these services, as used by User, is responsible for such data, through its services and operating systems.

12. Links to Third Party Sites

Third-party sites are included in Third-Party Services and Materials and as such are not under the control of Accessy, and Accessy is not responsible for the contents of any third-party sites, any links contained in third party sites, or any changes or updates to third-party sites.

13. Disclaimers

Accessy does not supply and is not responsible for any Third-Party Services and Materials. Any Third-Party Service and Material are subject to their own licenses, end-user agreements, privacy, and security policies, and/or terms of use. Accessy makes no warranty to and has no liability for Third-Party Services and Materials.

Except as stated herein, the Service, the App and any Documentation are provided to the User on an "as is" and "as available" basis.

Accessy does not warrant that use of the Service and the App will be error-free or uninterrupted. Accessy is not responsible for any hardware, mobile device, or software installed or used by the User or for the operation or performance of the Internet.

14. Liability

Accessy shall not be liable for any loss of profit, loss of use, loss of production, lost revenues, lost business or for any financial or economic loss or for any indirect or consequential damages whatsoever. Accessy does not accept liability

for Third-Party Service and Material. Accessy does not accept liability for any effects upon mobile devices, hardware, equipment, software, and computer programmes, or upon any electronic or radio systems in equipment, vehicles, or aircraft in the vicinity of the User, of any emissions or transmissions to, from, by or through the network and/or mobile devices and equipment.

Nothing herein shall limit or exclude either party's liability for; (a) Death or personal injury caused by its negligence, (b) fraud or fraudulent misrepresentation, and/or (c) any other liability that cannot be excluded by law.

15. Suspension of Service

Accessy, in its sole discretion, may suspend the User's use of the Service and/or the App until further notice; if the User violates/breaches any right and/or obligation under these General Terms, if it is revealed, or Accessy has reasonable ground for suspecting, that the User is using the Service, App or (on behalf of Accessy's customers) membership in Organizations, for illegal activities, fraud, situations involving potential threats to the physical safety of any person, or as otherwise required by law. Suspension is not a termination of subscription and membership, but merely a temporary suspension until relevant investigations have been performed.

Suspension does not exclude and is not related to the Organization's right to suspend or terminate the membership in accordance with the Organization's membership terms.

16. Term and termination

Accessy's obligation to provide the Service and the App and the User's obligation to abide to these General Terms shall take effect and commence on the Effective Date and shall continue to apply until terminated by a party in accordance with this Section.

A User may terminate the User's subscription(-s) to the Service and/or the App immediately and at any time. If You no longer wish to use our Service, the App and wish to close Your User Account, You can just unregister your User Account in the app or contact Accessy (support@accessy.se).

Accessy may terminate the User's subscription to the Service and/or the App immediately upon notice if; (a) the User is in material breach of its obligations under and pursuant to these General Terms, or (b) the User infringes any of Accessy's intellectual property rights, or challenges Accessy's ownership to or the validity of any intellectual property rights relating to the Service and/or the App, or (c) it is revealed, or Accessy has reasonable ground for suspecting, that the User is using the Service or App for illegal activities, fraud, situations involving potential threats to the physical safety of any person, or as otherwise required by law.

Please note that by deleting Your User Account, the identity, in other words, the mobile phone number registered in the Service, which is linked to Your Accesses, is also deleted.

Please note that if Your User Account is terminated all memberships linked to your User Account will automatically terminate.

If you only want to terminate a membership You can do so by ending it ("leaving it") by using Your App, or You can contact the Organization with which you have active membership and end it.

17. Winding up in the event of termination of the Service

Termination of the Service for a User will not only terminate the User's access to the Service and the App, but it will also automatically terminate all User's memberships and the possibility to access Organizations and Accesses.

18. Force majeure

Accessy will not be deemed in default, to the extent that performance of its obligations or attempts to cure any breach are delayed or prevented by reason of any event beyond the reasonable control of Accessy, including without limitation, any act of God, war and war-like situations, fire, earthquake, natural disaster, accident or act of government (in any case to the extent that such event is not due to, nor arises out of, the negligence of the party whose performance is delayed).

19. Notices

Any notice required or permitted hereunder shall be in writing and shall be given to the appropriate registered address or at such other address as the party may hereafter specify in writing. Such notice shall be deemed given; (a) if sent by

email with delivery receipt the same day, (b) upon personal delivery to the appropriate postal address, (c) 3 business days after the date of mailing if sent by certified or registered mail, or (d) 1 business day after the date of deposit with a commercial courier service offering next business day service with confirmation of delivery.

20. Severability

If any provision of the General Terms shall be found by any court or administrative body of competent jurisdiction to be invalid or unenforceable, such invalidity or unenforceability shall not affect the other provisions of the General Terms which shall remain in full force and effect.

21. Governing law and dispute

The Service, User Account and these General Terms and the rights and obligations of the parties pursuant thereto will be governed by the laws of Sweden, without regard to conflicts of law principles. The parties irrevocably agree that, subject as provided below, the courts of Sweden shall have exclusive jurisdiction in relation to any claim, dispute or difference concerning the Service and these General Terms (including the right to possible appeal), and any matter arising therefrom and irrevocably waive any right that they may have to object to an action being brought in those courts, or to claim that the action has been brought in an inconvenient forum, or that those courts do not have jurisdiction. Nothing in this Section shall limit the right of Accessy to, at any time, seek injunctive relief in the courts of any appropriate jurisdiction in the case of any breach or threatened breach or infringement of intellectual property rights.

Support Terms

The following support service is applicable to the use of Accessy's operated Service and App. Capitalized terms utilized in this document and not defined shall have the meaning set forth in the [General Terms and Conditions](#).

Accessy retains the right to make changes to these Support terms and conditions. Nevertheless, Accessy shall only make changes that do not negatively impact Users and shall apply generally to all Users. Detailed descriptions, specifications etc. for Accessy's Service and App will be provided by Accessy by general announcement.

1. General Support Coverage

Accessy's support team will be available (as specified in Section 2 below) to assist the User in the use of the Service and the App. Each incident will be allocated a unique reference number by Accessy's support team, and the User will be informed of this number for tracking purposes.

A support service means that a User can request for Accessy's remote assistance with matters relating to registration, access, use of the Service and the App, including assistance in the event of changes in the configurations of the Service and the App.

2. Support Availability

Any support request shall promptly be notified to Accessy per email to support@accessy.se or a webform on Accessy's [website](#) or by telephone set forth in the webform.

Support services for Service and the App shall be provided during Accessy's normal business hours (**Business Hours**).

- Monday – Friday (8 am – 5 pm the Swedish Time Zone) (Business Hours).
- Support services are provided primarily per email (support@accessy.se) and phone (+46 705 820 555).
- Accessy will use commercially reasonable efforts to respond to the User's support requests in connection with

the Service (Support Response).

3. Support Prerequisites

The User must provide the following information in the support request.

- (a) Name of the User
- (b) Email address and phone number to the User
- (c) Detailed description of support issue

Accessy Privacy Policy

This Privacy Policy (**Policy**) sets forth Accessy AB's policy with respect to information that can be associated with, or which relates to a person and/or could be used by Accessy to identify or localize a person (**Personal Data**) and that is collected from or about You as a private individual using Accessy's operated Access control services (**Service**), and Accessy's App (**App**). This Policy also describes how Accessy collects, uses, shares and secures Your Personal Data, and Your choices regarding the use, access, and correction of Your Personal Data.

The Policy creates the legal framework for processing of Personal Data in a manner compliant with all privacy and personal data legislation applicable to the Personal Data, including EU General Data Protection Regulation 2016/679 and any national laws adopted pertaining to this regulation (**GDPR**). The term includes binding guidelines, opinions, recommendations and decisions from supervisory authorities, courts, or other authority.

Separation of responsibilities

Even though all Your Personal Data is collected, stored and processed by and in the Service operated by Accessy, the GDPR requires a separation of responsibility between Accessy and each Organization (defined in [General Terms and Conditions](#)) in respect of the processing of Your Personal Data, based on the control over the relevant data. Under the GDPR Accessy is considered a *data controller* of some data and the Organization is considered a *data controller* of some data.

Accessy being a data controller

When registering for and using the Service and the App You need to provide certain Personal Data (name and phone number), which data Accessy will process for purposes of registration and use of Service/App (User Account Data as defined in [General Terms and Conditions](#)). For this Personal Data Accessy is a *data controller* pursuant to GDPR.

Accessy will also collect Service Data and store statistical data (other than Member Data) which may include information of Your use of the Service and App and may use location data (if allowed by you) linked to your use of the Service, as described in Section 1 below. Such data is used by Accessy for the operation and improvement of the Service and its functions. For this Personal Data Accessy is a *data controller* pursuant to GDPR.

Organization being a data controller

You need the App and to be registered for the Service to be able to use the Service. As described in more detail below, to be able to use the Service for certain Accesses You need to be included as a Member in the Organization administering the Accesses You want to use. When becoming a Member of an Organization, the Organization will include You in a certain registry in the Service dedicated to that Organization, by including Your name and phone number as already registered in the Service (Member Data as defined in [General Terms and Conditions](#)). The Personal Data also includes Your membership of the Organization. By becoming a Member of an Organization, the Organization is in control of Your Personal Data in the Member Data including Your Transaction Data related to that Organization's Accesses. For this Personal Data the Organization is a *data controller* pursuant to GDPR.

Your Personal Data related to Member Data is not covered by this Policy. When becoming a Member of an Organization, Your Personal Data related to Member Data will be treated in accordance with that Organization's membership terms and data privacy policy applicable to You.

Since You can be a Member in several Organizations, each Organization is the data controller of Your Personal Data

relating in Your Member Data (defined in [General Terms and Conditions](#)).

To accommodate that the Service process all Personal Data, including the Personal Data for which the Organization is the data controller, Accessy and each Organization has agreed, as part of the Organizations' subscription for the Service, that Accessy will, on behalf of the Organization, collect and process the Personal Data for which the Organization is responsible (Member Data). In this situation, subject to GDPR, Accessy is the Organization's *data processor*.

The Organization may also use the Service to access and process Your Transaction Data relating to the Organization's Accesses and membership. The purpose of accessing and processing such data is for the administration of Your memberships and Accesses, as further governed by the Organization's membership terms and data privacy policy applicable to You.

Scope of this Policy

This Policy set out the terms and conditions under which Accessy, as a *data controller*, shall treat Your Personal Data.

This Policy does not provide information of the processing for which the Organizations is a data controller. Instead, each Organization, as a data controller, shall treat Your Personal Data in accordance with what is set forth in the Organization's membership terms and privacy policy, which is provided to You when you become a Member in each Organization.

If You have questions or complaints regarding this Policy, or regarding Your Personal Data relating to the App, User Account, and the Service they should be directed to Accessy directly in its capacity of data controller of such data. Please write to us at atsupport@accessy.se.

If You have any questions or complaints regarding a membership or any specific questions or complaints regarding Your Personal Data related to certain Accesses under a specific Organization membership, please contact the Organization concerned.

1. Why does the Service collect and process Personal Data?

The Service is intended for use via mobile devices and downloaded application to gain Access (defined in [General Terms and Conditions](#)) to certain connected Assets in the Service. The person using the application (or **App**) is called a **User** (or **You**). Downloading and using the App is free of charge.

A User's Access or utilization of the Service requires the App and a registration for an individual account with Accessy (**Account**). For registration of the User Account the User is required to provide first name, last name, and mobile telephone number. When the User has registered the User Account, the User has the "**Access-tool**" (Accessy App + the User's mobile device) and is entitled to become a Member of one or several Organizations, either by applying for membership or by invitation. Membership is linked to your User-profile in the User Account. In other words, the User is identified by the mobile telephone number in the individual User Account.

When creating a User Account to use the Service the User also provides an explicit consent that Accessy may process the User's personal data in accordance with this Policy. By doing so the User also represent that the User is the owner of such User Account information or otherwise have the requisite consent to provide it to Accessy.

When a User has become a Member of a certain Organization the Organization will keep records to identify the User as a Member and the Organization will have access to and control Member's Access Data in the Service related to that Organization's Accesses. The Organization shall treat any such Personal Data in accordance with what is set forth in the Organization's privacy policy, which is provided to You when you become a Member in each Organization.

A User may also use the App to become a Customer, or represent a company being a Customer, or to be an Administrator of a specific Subscription. During this process the User will have to provide some personal data as the Customer's contact person or Administrator. Any such supplier personal data shall be treated in accordance with this policy.

The processing of Personal Data collected through the App, User Account and the Service is for the purpose of providing (administratively and electronically) and supporting the Service (such as keeping statistics, optimizing, uphold safety and security relating to the Service and to comply with legal requirements), as further described below.

Accessy will on its own account only host and process User's Personal Data obtained by the User becoming a User, and by the User using the Service (occasionally including location data), during and as a technical prerequisite for

Accessy to provide the Service. Accessy will, on behalf of Organizations, host and process Member Data and Access Data in the Service related to the Organizations' Accesses.

The lawful basis for Accessy to process User's Personal Data is User's explicit consent (when registering for User Account) and on the following lawful bases:

Performance of contract

- Provision of the Service (administratively and electronically) and supporting the Service (such as keeping statistics, optimizing, uphold safety and security relating to the Service and to comply with legal requirements).
- Billing and payment processes.
- Establish and defend legal claims.
- To ensure the security of our services and products, to detect and prevent use of the Service that is in violation of law or the terms and conditions for the Service. We also process data to prevent abuse of the Service, and to detect and prevent fraud, virus attacks etc.

Compliance with legal obligation

- To ensure the security of our services and products, to detect and prevent use of the Service that is in violation of law or the terms and conditions for the Service. We also process data to prevent abuse of the Service and Subscriptions, and to detect and prevent fraud, virus attacks etc.
- To meet our obligations under law, for example the Swedish Bookkeeping Act, and to response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

Legitimate interest

- To ensure necessary performance of functionality of the Service, to do technical enhancements and for improving the standard of the Service and security, to collect statistics for the Service, and to perform necessary log/register maintenance.
- To ensure adequate and correct communication with the User in relation to the Subscriptions. Communication calls, emails, and customer support online with our customer support may be recorded, analysed, and stored to train our employees and improve our ways of working.

User consent

- To ensure adequate and correct communication with the User in relation to the Subscriptions. Communication calls, emails, and customer support may be recorded, analysed, and stored to train our employees and improve our ways of working.
- Processing of different types of data to market our products and services. For this purpose, we may also compile statistics for analysis.

Accessy follow generally accepted standards to protect the Personal Data submitted to us, both during transmission and once it is received and stored. These security and privacy practices, including how we protect, collect, and use electronic data, text, messages, communications, or other materials submitted to and stored within the Service by You are found in Accessy's applicable [Accessy Data Security Standards](#).

Below You can find more detailed information on what data is collected and what it is used for.

User Account information

We collect and process Your Personal Data when You register for a User Account to access or utilize our Service, such as Your name (first name and last name) and mobile phone number, and for Customer Agreement also email address, to be able to provide our Service and to identify Your User Account in our Service.

Your mobile phone number is used to send You a SMS for activating Your User Account.

Your name is shared when requesting an Access and within Organizations You choose to join.

Your name, mobile phone number and email address is shared when creating and administrating Customer Agreements

and Subscriptions (as an Administrator).

Using the Service, Transaction Data and other statistics

While using our Service the Service collects information about Access Data, such as door operations, enabling charging stations or whatever operation that may be available from an Access. This information belongs to and is controlled by the Organization and in which You are a Member, and which enables Your Access.

When You request an Access, You will provide us with Your Personal Data and data of the requested Access. Your Personal Data will be available to the Administrator in the Organization who has the authorization to approve Your request. This information is stored if Your User Account is registered for use of the Service.

Accessy may also collect anonymous usage statistics to be used solely by Accessy to improve the Service and to find and fix problems and for improving safety and security when using the Service. We may also use mobile analytics software to allow us to better understand the functionality of our mobile versions of the App and the Service on Your mobile device. This mobile analytics software may record information such as how often You use the App, the events that occur within the App, aggregated usage, performance data, and where the application was downloaded from.

Accessy does not link any information that we store as usage statistics to any personally identifiable information that You submit for the mobile application.

Location data

You may choose to activate location data in Your mobile device to use the App to locate Your position (GPS positioning and Beacons) in relation to Accesses. The Service will then request permission to use Your location for displaying Accesses nearby in the App, but the Service does not (itself) process and store this location data, and as such this location data is not included in the Service, not covered by this Policy, and neither Accessy's nor the Organizations responsibility as a data controller. If You do not want to have Your location positioned, You can deactivate the location positioning function in Your mobile device.

The Service may also, occasionally and depending on whether a particular Organization has activated this functionality, use Access location data within the Service. The Access location data is a special functionality or configuration to Accesses used if the Organization requires proximity for Accesses (not remote Access). The Access location data together with the geographical position of an Access will indicate a User's performed Access at a certain time at a certain geographical place. Such Access location data is included in the Service and will be stored in the Service related to Accesses and as such covered by this Policy and Accessy's responsibility. This location data processed in the Service is not controlled or processed by the Organizations.

App

When registering an App to Your User Account and downloading the App to Your mobile device, the Service automatically collects information on the type of device You use, and the operating Service version. If the App is running in iOS, You will also provide the Service with information on the device name such as "Eric's iPhone".

Other

As for most websites and services delivered over the Internet, Accessy gathers certain information and stores it in log files when You interact with our websites and Service. This information includes internet protocol (IP) addresses as well as browser type, internet service provider, URLs of referring/exit pages, operating system, date/time stamp, information You search for, locale and language preferences, identification numbers associated with Your devices, Your mobile carrier, and system configuration information. Occasionally, Accessy connects Personal Data to information gathered in our log files as necessary to improve our Websites and the Service. In such a case, we will treat the combined information in accordance with this Policy.

2. Will collected information be shared?

Accessy only shares Service data, including Personal Data, with our subscribing Organizations and their Administrators (see description below), and third-party service providers that Accessy uses to provide hosting for and maintenance of our Service, App development, backup, storage, payment processing, analytics, and other services for Accessy. These third-party service providers may have access to or process Your Personal Data for the purpose of providing services

to Accessy.

All information about You and about Your User Account Data, Accesses and Access Data will, as a technical necessity, be automatically shared with the Organization that You belong to as a Member and its Administrators, for the purpose of administering Your membership and Your Accesses. Each Organization's use and processing of such data will be within the scope of the Service and Your membership with that Organization. The Organization's use of such data will be in accordance with each Organization's membership terms and data privacy policy which are provided to You when becoming a member of each Organization.

Accessy does not permit any third-party to use Your Personal Data for marketing purposes or for any other purpose than in connection with the services they provide to Accessy.

In certain situations, Accessy may be required to disclose Your Personal Data, or specific Access Data, in response to lawful requests by public authorities, including to meet national security or law enforcement requirements. Accessy may disclose such data to respond to subpoenas, court orders, or legal process, or to establish or exercise our legal rights or defend against legal claims. Accessy may also share such information to the extent necessary to investigate, prevent, or act regarding illegal activities, suspected fraud, situations involving potential threats to the physical safety of any person, violations of our applicable subscription/license agreements, or as otherwise required by law.

Accessy may also share Personal Data with other third parties when we have Your consent to do so.

3. Will transfer of Personal Data occur?

All data in the Service is processed within the European Economic Area (EEA).

Accessy is currently using Microsoft Azure¹ managed services for data processing and data storage (IaaS), in Microsoft Azure's servers in North and West Europe (Ireland and Netherlands). However, Microsoft Azure's processing and storage procedures may include that Service Data and/or Personal Data may be transferred outside of the EU/EEA within the Accessy's use of the service.

Having our IT infrastructure with Microsoft Azure (as Accessy's sub-processor) provides security that is designed and managed in alignment with best security practices and a variety of IT security standards.

Having our service operate on Microsoft Azure ensures that we can work in a manner which is certified under several global compliance programmes which underlines best practices in terms of data centre security.

All data in the Service which is stored and managed in and by Microsoft Azure's managed services for data processing and data storage (IaaS) can only be processed by using the Accessy Service.

All communication and transfer of personal data to and from (to Accessy) Microsoft Azure is encrypted. We use best practices in terms of encryption and security.

For more information about Microsoft Azure managed services for transfer of personal data outside of the EU and reasons for why Microsoft Azure may share personal data may be found [here](#) and [here](#):

Accessy is currently using Fortnox's services for billing processing. Your Personal Data may be included in the billing data (on the invoice or in accompanying specifications) for reference purposes. Fortnox's processing do not include that any Personal Data is transferred outside of the EU/EEA. More information about Fortnox's services and privacy policy may be found [here](#).

4. How long do we keep data?

Accessy shall only collect and process User's Personal Data for as long as needed for Accessy to perform its contractual obligations to You, to comply with legal obligations, to resolve disputes, to preserve legal rights, or to enforce agreements.

Accessy shall only retain Your Transaction Data constituting Personal Data for 3 months after performed transaction. Any such Transaction Data constituting Personal Data may be retained longer for reasons described in (a) – (j) above, but then such data will be kept in an aggregated and anonymized way.

Once Your User Account is terminated, we will automatically delete or anonymize all Your User Account Data and Transaction Data within 3 months from User Account-closure (see Section 5), in accordance with the capabilities of the Service in accordance with GDPR Article 28(3)(g). Please note that data may be retained longer for reasons described

herein, but then such data will be kept in an aggregated and anonymized way.

5. How to terminate the Service, the User Account and delete the App

If You no longer wish to use our Service, the App and wish to close Your User Account, You can simply deactivate Your User Account by using the App and You can delete the App from Your mobile device., or You can contact Accessy and request to have Your User Account deactivated and deleted, please email support@accessy.se.

6. What if a data security breach?

Accessy has implemented and maintains appropriate technical and organizational measures to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access (a **Data Security Breach**), taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, so as to ensure a level of security appropriate to the risks represented by the processing and the nature of the Personal Data to be protected, including data security consistent with the [Accessy Data Security Standards](#).

If You want to report a Data Security Breach, please contact us via support@accessy.se.

7. What are Your rights?

You have the right to be informed of what data Accessy processes about You when using the Service and the App, which is covered by this Policy. Furthermore, You have the right to review Your data. (All Your User Account Data and Organization Data will be shown and can be handled by You in Your App.)

If You believe that the information about You that Accessy process and store is incorrect, then You have the right to have it amended and, in some cases, deleted.

When the processing of Personal Data is based on Your consent, You have the right to withdraw that consent at any time. The withdrawal of Your consent does not affect the lawfulness of processing based on consent before the withdrawal. If You wish to exercise any of Your rights, please contact us via support@accessy.se.

Please note that if You request that Accessy restricts or erases Your Personal Data or if You withdraw Your consent, this may lead to that the Service and App no longer can be fully provided to You.

You have the right to complain to a Data Protection Authority about our collection and use of Your Personal Data. For more information, please contact Your local data protection authority in the EEA. If You are in Sweden, you may complain to [Integritetsmyndigheten](#).

8. Will this Policy change?

Should European Parliament and/or the Council pass new regulations and/or issue any guidelines which contains terms that conflict with those used in this Policy, Accessy reserves the right to change this Policy from time to time to make it compliant with any such new legislation or guideline.

Accessy Data Security Standards

This Data Security Standard policy (**Policy**) sets forth Accessy AB's, a Swedish corporation with address Södra Förstadsgatan 2, 211 43 Malmö, Sweden (**Accessy**) technical and organizational security measures for the processing of Service Data and Personal Data to ensure a level of security appropriate to risks (**Security Standards**). These Security Standards apply to all Personal Data that Accessy receives and process using the Accessy operated services (**Service**) and Accessy's App.

1. Access and access control

Accessy has a Service for Access control; to give the right person the right level and scope of access to the Service and connected Assets in the Service. Accessy has procedures for how access permissions in the Service are granted and

removed. Accessy have certificate-based authentication checks and all authentication information is stored securely.

2. Physical access controls

Accessy takes reasonable measures to prevent physical access and prevent unauthorized persons from gaining access to Service data or ensure third parties operating data centres on its behalf are adhering to such controls.

3. Service access controls

Accessy takes reasonable measures to prevent Service data from being used without authorization. These measures vary based on the nature of the data processing undertaken and may include, among other;

- (a) controls,
- (b) authentication via passwords and/or two-factor authentication, and
- (c) log of access on several levels.

All access is logged and audited for suspicious/anomalous behaviour.

4. Service Data access controls

Accessy takes reasonable measures to provide that;

- (a) Service data is accessible and manageable only by properly authorized staff and authorized Organizations,
- (b) direct database query access is restricted, and application access rights are established and enforced to ensure that persons and Organizations (and its Administrators) entitled to use a data processing system only have access to the Service data to which they have privilege of access, and
- (c) Service data cannot be read, copied, modified, or removed without authorization while processing.

5. Transmission controls

Accessy takes reasonable measures to ensure that it is possible to check and establish to which entities the transfer of Service data by means of data transmission facilities is envisaged so that Service Data cannot be read, copied, modified, or removed without authorization during electronic transmission or transport.

6. Input controls

Accessy use commercial best efforts to provide that it is possible to check and establish whether and by whom Service data has been entered into data processing systems, modified, or removed.

Accessy takes reasonable measures to ensure that;

- (a) the Service data source is under the control of relevant Data Controller, and
- (b) Service data integrated into the Service is managed by secured transmission from Accessy for interactions with Accessy's User Interface (UI) or Application Programming Interface (API).

7. Data backup

Back-ups of the databases in the Service are taken on a regular basis, are secured to ensure that Service data is protected against accidental destruction or loss. Accessy have documented procedures for recovery of data.

8. Logical separation

Service data from different customers and users is logically segregated on systems managed by Accessy to ensure that Service data that is collected by different customers and users is segregated from one another.

9. Physical safety

Equipment, portable data media and the like that are not under the supervision of the Service data tree are locked to be protected against unauthorized use, influence, and theft.
