

## Data Security for App based Client management system Makerble

### GDPR Compliance

At Makerble we give you the tools to comply with GDPR. In relation to your clients' personal data, Makerble is the data processor and your organisation is the data controller.

#### 1. CONSENT

- The General Data Protection Regulation requires that you get consent from the people whose data you store.
- When you store a person's information on Makerble, they are stored as a **Contact**.
- One of the fields within the Contact form is called Consent and it allows you to record **whether you have obtained that person's consent**. Here's how it works in practice:
  - If you ask people to sign a paper consent form, you can **upload that signed form** to their Contact record on Makerble
  - Using the **Date of Consent** field on Makerble, you can record the date that consent was granted
  - Using the **Who Consent was Granted by** field on Makerble, you can record whether it was the person themselves, a parent, guardian or someone else who gave that consent.
  - You can easily **add additional consent fields** to your Contact forms.

#### 2. RESTRICTED ACCESS TO SENSITIVE PERSONAL DATA

- The GDPR requires that organisations restrict access to people's Personal Data.
- On Makerble, you can customise the level of access that each user has to each beneficiary, client, service user and person you work with.

#### 3. DATA STORAGE

- When you use Makerble, your data is stored on servers housed in secure data centres located in London, England.
- The data is encrypted at REST and stored in AWS S3 buckets.
- Your data is never sold.

#### 4. DATA RIGHTS

- Under the GDPR, people have rights related to the data you store about them. Among those rights are the right to request that you delete all data you store about them, show them the data you store about and move the data that you store about them to another organisation.
- Makerble gives you the tools to comply with these regulations.
  - Deletion: in the event that one of your beneficiaries requests that you delete the data you store about them, you can easily do this on Makerble by pressing the **Delete** Contact button.
  - Access: in the event that one of your beneficiaries requests that you give them access to the data you store about them, you can **print** their beneficiary record from the Contact profile page.
  - Portability: in the event that one of your beneficiaries requests that you move the data you have about them to another organisation, you can give that organisation **access** to the Contact profile of that beneficiary.

## 5. LEGAL BASIS

- Under the GDPR you must record the legal basis for which you are processing someone's personal data.
- On Makerble we support you to do this by enabling you to select the legal basis on which you are storing information about the beneficiaries you work with. In many cases it will be Consent or Legitimate Interest.
- There are six possible legal bases on which you can process someone's personal data.
  - **(a) Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.
  - **(b) Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
  - **(c) Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).
  - **(d) Vital interests:** the processing is necessary to protect someone's life.
  - **(e) Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
  - **(f) Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

For additional guidance on how to adhere with the General Data Protection Regulations, contact our Data Protection Officer by email:

dataprotection@makerble.com. Additional resources are available from The Information Commissioner's Office: <https://ico.org.uk/>

## PRIVACY POLICY

**Makerble acts as a Data Processor in some instances and as a Data Controller in others. Read on to find out how Makerble is responsible for your data and how we treat it.**

	<b>If you are an Organisation</b>	<b>If you receive help from an Organisation that uses Makerble</b> E.g. you are a Participant / Beneficiary / Client of an Organisation	<b>If you are have your own personal Makerble account</b>
<b>Our role</b>	Makerble is your Data Processor	The organisation that helps you is your Data Controller	Makerble is your Data Controller

### **If you receive help from an organisation that uses Makerble**

Makerble has been designed to make it easier for organisations that help groups of people (charities, nonprofits, NGOs, social enterprises, providers of social services, schools and other bodies) to create a bigger difference in the world. Makerble does this by enabling those organisations to record the difference that they are making on each of their projects and keep track of whether the work they do is having a positive impact on the lives of people like you who they are set up to help. As a result, those organisations need to store information about you and the projects that they are involving you in. This section of the Makerble privacy policy outlines how that information is stored

If you do not have a personal account on Makerble

**The role of Makerble:** If you do not have your own personal account on Makerble, Makerble is not your data controller. The organisation whose projects you are involved with is your data controller. This means that you need to contact them to find out how they store your information. Makerble simply acts as the Data Processor for that organisation which means that they use our system to store and process the data they collect. That being said, there is some information which we can give you as an overview of what information the organisation is likely to be storing.

	<b>Information collected</b>	<b>How and why it is collected</b>
<b>Information that the organisations helping you are able to collect about you</b>	Your Name will usually be recorded The organisation helping you has the ability to collect additional information about you which is stored on your Contact Record	It is likely that the organisation is collecting this information about you so that they can improve the quality of the services that they provide to you.

If you do have a personal account on Makerble

If you receive help from an organisation and you do have a personal account on Makerble, Welcome! Because you have a personal account on Makerble there are two sets of information that are stored about you; in summary, the information that is for each of the Organisations whose projects you are involved with and separately, the information that enables Makerble to provide you with a great experience of the platform. We refer to people who receive help from an organisation while having their own personal account on Makerble, "Active Participants".

Scenarios	Who your Data Controller is in each scenario	
	The organisation whose projects you are involved with is the Data Controller	Makerble is the Data Controller
<p>When you sign up for Makerble and create your own profile, you are asked to enter the following information:</p> <ul style="list-style-type: none"> <li>Your Name</li> <li>Email Address</li> </ul> <p>And you can optionally add in</p> <ul style="list-style-type: none"> <li>Date of Birth</li> <li>Profile Picture</li> <li>Gender</li> <li>Occupation</li> </ul> <p>This information is used to give you a personalised experience of the platform, for example, displaying your name and profile picture to you when you login.</p>	No	Yes
<p>When you link your Makerble Account to each of the organisations whose projects and services you are involved in, it means that you can now create stories and survey responses related to the projects of theirs that you are involved with. Information that is collected in your stories and survey responses can include:</p> <ul style="list-style-type: none"> <li>Text that you add</li> <li>Your choice of pictures and attachments</li> <li>Your answers to each organisation's questions</li> <li>Location of where the story was written</li> </ul> <p>The organisation whose projects you are involved with is the Data Controller in this case and can provide with you more information on how and why they use this data.</p>	Yes	No
<p>Makerble collects usage data from all of its users. This includes:</p> <ul style="list-style-type: none"> <li>how often people sign in, when they sign in, which type of devices they sign in from, the pages people get stuck on</li> </ul> <p>This information is collected so that Makerble can understand how we can improve the platform. For example if we can see a trend that people are having problems with a certain page, our engineers can then fix that page. The organisation that supports you will also find this information useful.</p>	Yes	Yes

## MAKERBLE AS A DATA CONTROLLER

### If you are someone with a personal account on Makerble

Makerble is a tool that has been designed to make it easier for you to make a positive difference in the world, whether that is through the organisation you work or volunteer for, the organisations you donate to, sign petitions for, create stories for or donate to. Dependent on how the organisation has setup their Makerble account, that organisation will also act as your Data Controller as well as Makerble.

- **Introduction to the Privacy Policy (updated in line with The General Data Protection Regulations)**

Make Worldwide Limited (“**Makerble**”, “**we**” and “**us**”) is committed to protecting your privacy when you are using [www.makerble.com](http://www.makerble.com), the Makerble app or any other services provided to you by us (the “**Services**”). This Privacy Policy explains the following:

- what information we may collect about you;
- how we use the information we collect about you;
- whether we will share your details with anyone else;
- how you can instruct us if you prefer to limit the use of that information;
- the procedures that we have in place to safeguard your privacy; and
- the use of cookies on the Services and how you can reject those cookies.

By using the Services or by submitting information to us, you signify your consent to the collection, use and sharing of your personal information in accordance with this Privacy Policy.

If you have any requests concerning your personal information or any queries with regard to these practices please contact us using the contact details at the end of this Privacy Policy.

At Makerble we have adopted a Privacy by Design approach which means that we have built privacy controls into Makerble itself to give you as much control over your data as possible.

***If you do not agree with this Privacy Policy, you must not use the Services or submit any information to us.***

- **What information will we collect?**

When you download, access, visit or use the Services we may receive and collect personal information about you. This is information that relates to and identifies you and may include (but is not limited to): your name, postal address, e-mail address, telephone number, details of payment cards used, Facebook and/or Twitter profile picture, gender, and usernames that you provide as part of you linking any of your Facebook and Twitter accounts to your use of the Services.

By submitting these details you enable us to provide you with the services, activities or online content you select.

We also use cookies and collect IP addresses (this is a number that can uniquely identify a specific computer or other device on the internet) from all visitors to the Services.

The data is retained for as long as you have an account with us.

- **How do we use the information we collect?**

The primary legal basis for which we will use your personal information is that processing is necessary for the purposes of the legitimate interests pursued by Makerble as the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Here are some of the specific ways in which we use your data:

- providing and personalising our services;
- dealing with your enquiries and requests;
- compiling your membership profile;
- to personalise the way the Services are presented to you;
- providing you with information about our services, activities and online content;
- to analyse and improve your use of the Services;
- for “service administration purposes” so we may contact you for reasons related to the Services you have signed up for; and

- for marketing purposes.

We may also gather information and statistics for the purpose of monitoring usage of the Services and may provide such aggregate information to third parties. These statistics will not include information that can be used to identify you.

If you choose to post messages in one of the forums or other message areas, we may collect the information you provide to us and retain this information to resolve disputes, for research purposes, to provide customer support and troubleshoot problems, as permitted by law.

If you stop using the Services or your permission to use the Services is terminated, we may continue to use and disclose your personal information in accordance with this Privacy Policy (as amended from time to time) and as permitted by law.

If you wish us to stop contacting you with information in connection with the Services, please send us an email using the contact details at the end of this Privacy Policy.

- **Will we share information with anyone else?**

We will keep your information confidential except where we are required or permitted to disclose it by law (for example to government bodies and law enforcement agencies or in response to other legal or regulatory requests).

We may also share your information with the following people for the purpose of processing your information:

- our employees;
- our affiliates and the charities we work with;
- our group companies and their employees;
- successors in title to our business;
- third party consultants, contractors or other service providers who may access your personal information when providing services to us (for example, advertisers); and
- auditors or contractors or other advisers auditing, assisting with or advising on any of our business purposes.

We will require these third parties to comply strictly with our instructions and request that they do not use your personal information for their own business purposes (unless you have specifically consented to this).

- **What rights do you have to see what information we collect about you?**

Under the Data Protection Act and the General Data Protection Regulation you have the right to request a copy of the personal information we hold about you and to have any inaccuracies corrected.

Before responding to any request, we will require proof of your identity.

Please send all requests for information to the contact details provided at the end of this Privacy Policy.

You have the right to withdraw your consent at any time.

You have the right to lodge a complaint with a supervisory authority, for example with the Information Commissioners Office in the United Kingdom.

If information which we have about you is incorrect, you have the right for it to be corrected. You also have the right for information about you to be deleted. In summary, you have all of these rights:

- **To be informed**
- **Of access** – you have the right to access any data we've processed of yours
- **Of rectification** – you can rectify incomplete or inaccurate data

- **To erasure** – you can request that we delete your data
- **To restrict processing** – you can block the processing of your data
- **To data portability** – you can reuse your data for other services
- **To object** – you can object to the processing of your data
- **In relation to automation** – you can object from automated decision-making being done based on your data
- **Will you be contacted for marketing purposes?**

We will only contact you for marketing purposes, or to promote new services, activities or online content if you have consented to this by “opting-in”.

You can opt-out of receiving any communications by contacting us using the contact details at the end of this Privacy Policy.

- **Cookie Policy**

- What is a cookie?

A cookie is a small piece of information sent by a web server to a web browser, which enables information about your browsing patterns to be collected. This then allows us to tailor the Services to your interests. Cookies are widely used in order to make websites work, as well as to provide business and marketing information to the owners of the site.

<http://www.allaboutcookies.org> is a good site to visit if you want to find out more about the use of cookies.

- How do we use cookies on the Services?

We use cookies on the Services for the following purposes:

- Technical reasons, for example to balance website traffic to ensure that you receive a consistent and reliable service.
- To enhance the ease of use of the Services users, for example remembering your preferences or login details.
- Gathering statistics on how users access and use the Services.
- Marketing, for example, to allow advertisers to display appropriate advertising and track its effectiveness. You can opt-out of receiving any marketing communications by contacting us using the contact details at the end of this Privacy Policy.
- Other cookies.

We may sometimes embed links to other websites or photos and video content from websites such as YouTube and Flickr. As a result, when you visit a page containing such content, you may be presented with cookies from these websites. We do not control the dissemination of these cookies and you should check the relevant third party's website for more information.

- Can you turn off these cookies?

You can change your browser settings to turn off cookies. However, if you do change your settings and block certain cookies, this means that certain personalised features cannot be provided to you and you may not be able to have the full advantages of the Services' features.

- **What if you are accessing other websites through the Services?**

The Services may contain hyperlinks to other websites owned and operated by third parties. These third party websites will have their own privacy policies, and are also likely to use cookies, so we recommend you look at these policies before using the third party website. As these websites are outside of our control we cannot accept any responsibility or liability for the privacy practices used by the third parties and the use of these websites is at your own risk.

- **How secure is your information?**

Please be aware that communications over a network are not secure unless they have been encrypted and your communications may route through a number of countries before being delivered. We cannot accept responsibility for any unauthorised access or loss or personal information that is beyond our control.

We believe that we have appropriate policies, rules and technical measures in place to protect your personal information that is under our control from unauthorised access, improper use or disclosure, unauthorised modification, unlawful destruction or accidental loss. All of our employees and data processors that have access to, or are associated with, the processing of your personal information are obliged to respect the confidentiality of the information.

Owing to the global nature of the Internet, the information you provide may be transferred in transit to countries outside of the European Economic Area. By using the Services you accept that your information may be transferred outside of the EEA and consent to this. Although some countries outside of the EEA may not have similar privacy protections in place, we will take adequate steps to ensure the security of your information should it be transferred outside of the EEA.

- **How do you give consent to the use of your information under this Privacy Policy?**

By submitting any personal information to us you consent to the use of the information as set out in this Privacy Policy.

We reserve the right to amend or modify this Privacy Policy and if we do so we will post the changes on this page. You will need to check this Privacy Policy every time you submit information to us to ensure you are aware of any changes made. Subsequent use of the Services will signify that you agree to the changes.

- **Can you give consent if you are a user who is aged 16 or under?**

If you are aged 16 or under you will need to get your parent/guardian's permission before you provide us with any personal information. If you do not have this permission, you are not allowed to provide us with any personal information.

- **How do you contact us?**

If you have any questions or queries about this Privacy Policy or would like to request a copy of your personal information please contact [hello@makeworldwide.com](mailto:hello@makeworldwide.com)

The data protection officer is Matt Kepple who can be contacted on [matt@makeworldwide.com](mailto:matt@makeworldwide.com) or by post at 83 Ducie Street, Manchester, M1 2LQ, England. The data controller when you create a personal account on Makerble is Makerble and you can contact Makerble at 83 Ducie Street, Manchester, M1 2LQ, England.

- **Third Parties**

Any Personal Data that we collect from you will be stored at a secure cloud data centre hosted by Amazon and located outside the European Economic Area. By submitting the Personal Data, you agree to this storing. We may share your Personal Data with other third party service providers whom we employ to perform tasks on our behalf, but these service providers do not have any right to use the Personal Data that we share with them in a manner other than that necessary to assist us. These service providers include CRM solution providers (such as HubSpot), payment processing providers (such as Stripe), email service providers (such as Mailchimp), website analytics providers (such as Google Analytics), and other service providers from time to time. Some of these service providers may process your Personal Data outside the European Economic Area. We will take all steps reasonably necessary to ensure that your Personal Data is treated securely and in accordance with these Terms



and with the requirements for international data transfers under EU law, and by submitting the Personal Data, you agree to such sharing.

- **If you use the Makerble Marketplace**

We created the Makerble Marketplace ([www.makerble.com/explore](http://www.makerble.com/explore)) to give you a way to make a difference in the world without having to be worried that your data would be used to send you marketing and fundraising materials without your consent. Organisations that are changing the world (charities, social enterprises, nonprofits, NGOs, etc) often rely on donations to stay afloat, but we recognise that you as an individual only want to be contacted by the organisations whom you have explicitly asked to be contacted by.

For this reason, if you use the Makerble Marketplace as a way to find **new** organisations to support, you can be confident that those organisations will not contact you without your permission. That is the freedom that the Makerble Marketplace gives you. You can follow, fund, comment on stories and sign the petitions of projects and you will not be contacted independently by the organisations running those projects.

On Makerble you control the notifications you receive. You can control them from your Notification Settings page once you are signed in.

<b>Communications you can receive within Makerble.</b> You can also control whether you receive some of these notifications.	<b>Communications independent of Makerble</b>
<p>When we say notifications we are referring to Emails, Web Notifications, Chrome Notifications and/or Push Notifications</p> <ul style="list-style-type: none"> <li>• Notification when a new story has been written by a project you follow or donate to</li> <li>• Notification when an impact milestone has been reached</li> <li>• Notification when you receive a private message from another user on Makerble. (Technically it is possible for employees of Organisations on Makerble could use this system to proactively message you. If you find that this is happening too much, please report it to us as we do not want to restrict communications but we also do not want people to be contacted by lots of people they do not know.</li> <li>• Notification when someone comments on a story you wrote or a story you previously commented on</li> </ul>	<p>For example a newsletter from a charity's email address.</p> <p>This will <b>not</b> happen when you are using Makerble Marketplace unless you specifically opt-in to receive additional communications from that charity</p>

When you use Makerble Marketplace, Makerble is the Data Controller

<b>Information collected and how as well as why it is used</b>	<b>The organisation whose projects you support by</b>	<b>Makerble is the Data Controller</b>
	<ul style="list-style-type: none"> <li>• <b>donating,</b></li> <li>• <b>following,</b></li> <li>• <b>signing petitions</b></li> <li>• <b>commenting on</b></li> </ul> <p><b>is the Data Controller</b></p>	

<p>When you use the Makerble and create your own profile you are asked to enter the following information:</p> <ul style="list-style-type: none"> <li>• Your Name</li> <li>• Email Address</li> </ul> <p>And you can optionally add in</p> <ul style="list-style-type: none"> <li>• Date of Birth</li> <li>• Profile Picture</li> <li>• Gender</li> <li>• Occupation</li> </ul> <p>This information is used to give you a personalised experience of the platform, for example, displaying your name and profile picture to you when you login.</p>	No	Yes
<p>When you donate, the amount of money that you donate is stored. Makerble also records the causes that you are interested in. This is so that the Makerble algorithm can optimise your experience of the platform to show you projects, people, stories and opportunities from causes and interests that we think you will enjoy</p>	No	Yes

## MAKERBLE AS A DATA PROCESSOR

### Makerble’s Agreement with Data Controllers

This Makerble Agreement with Data Controllers (“ADC”), that includes the Standard Contractual Clauses adopted by the European Commission, as applicable, reflects the parties’ agreement with respect to the terms governing the Processing of Personal Data under the Makerble Terms of Service for [Organisations](#) and for [Users](#).

The term of this ADC shall follow the term of the Terms and Conditions. Terms not otherwise defined herein shall have the meaning as set forth in the Terms and Conditions.

THIS ADC INCLUDES:

- (i) Standard Contractual Clauses, attached hereto as EXHIBIT 1.
  - (a) Appendix 1 to the Standard Contractual Clauses, which includes specifics on the Personal Data transferred by the data exporter to the data importer.
  - (b) Appendix 2 to the Standard Contractual Clauses, which includes a description of the technical and organizational security measures implemented by the data importer as referenced.
- (ii) List of Sub-Processors, attached hereto as EXHIBIT 2.

### 1. Definitions

“Controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

“Data Protection Law” means all applicable legislation relating to data protection and privacy including without limitation the EU Data Protection Directive 95/46/EC and all local laws and regulations which amend or replace any of them, including the GDPR, together with any national implementing laws in any Member State of the European Union or, to the extent applicable, in any other country, as amended, repealed, consolidated or replaced from time to time. The terms “process”, “processes” and “processed” will be construed accordingly.

“Data Subject” means the individual to whom Personal Data relates.

“GDPR” means the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

“Instruction” means the written, documented instruction, issued by Controller to Processor, and directing the same to perform a specific action with regard to Personal Data (including, but not limited to, depersonalizing, blocking, deletion, making available).

“Personal Data” means any information relating to an identified or identifiable individual where such information is contained within Customer Data and is protected similarly as personal data or personally identifiable information under applicable Data Protection Law

“Personal Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

“Processing” means any operation or set of operations which is performed on Personal Data, encompassing the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction or erasure of Personal Data.

“Processor” means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller.

“Standard Contractual Clauses” means the clauses attached hereto as Exhibit 1 pursuant to the European Commission’s decision (C(2010)593) of 5 February 2010 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

## **2. Details of the Processing**

a. Categories of Data Subjects. Controller’s Contacts and other end users including Controller’s employees, contractors, collaborators, customers, prospects, suppliers and subcontractors. Data Subjects also include individuals attempting to communicate with or transfer Personal Data to the Controller’s end users.

b. Types of Personal Data. Contact Information, the extent of which is determined and controlled by the Customer in its sole discretion, and other Personal Data such as navigational data (including website usage information), email data, system usage data, application integration data, and other electronic data submitted, stored, sent, or received by end users via the Subscription Service.

c. Subject-Matter and Nature of the Processing. The subject-matter of Processing of Personal Data by Processor is the provision of the services to the Controller that involves the Processing of Personal Data. Personal Data will be subject to those Processing activities as may be specified in the Terms and Conditions and an Order.

d. Purpose of the Processing. Personal Data will be Processed for purposes of providing the services set out and otherwise agreed to in the Terms and Conditions and any applicable Order.

e. Duration of the Processing. Personal Data will be Processed for the duration of the Terms and Conditions, subject to Section 4 of this ADC.

## **3. Customer Responsibility**

Within the scope of the Terms and Conditions and in its use of the services, Controller shall be solely responsible for complying with the statutory requirements relating to data protection and privacy, in particular regarding the disclosure and transfer of Personal Data to the Processor and the Processing of Personal Data. For the avoidance of doubt, Controller’s instructions for the Processing of Personal Data shall comply with the Data Protection Law. This ADC is Customer’s complete and final instruction to Makerble in relation to Personal Data and that additional instructions outside the scope of ADC would require prior written agreement between the parties. Instructions shall initially be

specified in the Terms and Conditions and may, from time to time thereafter, be amended, amplified or replaced by Controller in separate written instructions (as individual instructions).

Controller shall inform Processor without undue delay and comprehensively about any errors or irregularities related to statutory provisions on the Processing of Personal Data.

#### **4. Obligations of Processor**

**a. Compliance with Instructions.** The parties acknowledge and agree that Customer is the Controller of Personal Data and Makerble is the Processor of that data. Processor shall collect, process and use Personal Data only within the scope of Controller's Instructions. If the Processor believes that an Instruction of the Controller infringes the Data Protection Law, it shall immediately inform the Controller without delay. If Processor cannot process Personal Data in accordance with the Instructions due to a legal requirement under any applicable European Union or Member State law, Processor will (i) promptly notify the Controller of that legal requirement before the relevant Processing to the extent permitted by the Data Protection Law; and (ii) cease all Processing (other than merely storing and maintaining the security of the affected Personal Data) until such time as the Controller issues new instructions with which Processor is able to comply. If this provision is invoked, Processor will not be liable to the Controller under the Terms and Conditions for any failure to perform the applicable services until such time as the Controller issues new instructions in regard to the Processing.

**b. Security.** Processor shall take the appropriate technical and organizational measures to adequately protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data, described under Appendix 2 to the Standard Contractual Clauses. Such measures include, but are not be limited to:

- i. the prevention of unauthorized persons from gaining access to Personal Data Processing systems (physical access control),
- ii. the prevention of Personal Data Processing systems from being used without authorization (logical access control),
- iii. ensuring that persons entitled to use a Personal Data Processing system gain access only to such Personal Data as they are entitled to accessing in accordance with their access rights, and that, in the course of Processing or use and after storage, Personal Data cannot be read, copied, modified or deleted without authorization (data access control),
- iv. ensuring that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media, and that the target entities for any transfer of Personal Data by means of data transmission facilities can be established and verified (data transfer control),
- v. ensuring the establishment of an audit trail to document whether and by whom Personal Data have been entered into, modified in, or removed from Personal Data Processing systems (entry control),
- vi. ensuring that Personal Data is Processed solely in accordance with the Instructions (control of instructions),
- vii. ensuring that Personal Data is protected against accidental destruction or loss (availability control).

Processor will facilitate Controller's compliance with the Controller's obligation to implement security measures with respect to Personal Data (including if applicable Controller's obligations pursuant to Articles 32 to 34 (inclusive) of the GDPR), by (i) implementing and maintaining the security measures described under Appendix 2, (ii) complying with the terms of Section 4.4 (Personal Data Breaches); and (iii) providing the Controller with information in relation to the Processing in accordance with Section 5 (Audits).

**c. Confidentiality.** Processor shall ensure that any personnel whom Processor authorizes to process Personal Data on its behalf is subject to confidentiality obligations with respect to that Personal Data. The undertaking to confidentiality shall continue after the termination of the above-entitled activities.

**d. Personal Data Breaches.** Processor will notify the Controller as soon as practicable after it becomes aware of any of any Personal Data Breach affecting any Personal Data. At the Controller's request, Processor will promptly provide the Controller with all reasonable assistance necessary to enable the Controller to notify relevant Personal Data Breaches to competent authorities and/or affected Data Subjects, if Controller is required to do so under the Data Protection Law.

**e. Data Subject Requests.** Processor will provide reasonable assistance, including by appropriate technical and organizational measures and taking into account the nature of the Processing, to enable Controller to respond to any request from Data Subjects seeking to exercise their rights under the Data Protection Law with respect to Personal Data (including access, rectification, restriction, deletion or portability of Personal Data, as applicable), to the extent permitted by the law. If such request is made directly to Processor, Processor will promptly inform Controller and will advise Data Subjects to submit their request to the Controller. Controller shall be solely responsible for responding to any Data Subjects' requests. Controller shall reimburse Processor for the costs arising from this assistance.

**f. Sub-Processors.** Processor shall be entitled to engage sub-Processors to fulfil Processor's obligations defined in the Terms and Conditions only with Controller's written consent. For these purposes, Controller consents to the engagement as sub-Processors of Processor's affiliated companies and the third parties listed in Exhibit 2. For the avoidance of doubt, the above authorization constitutes Controller's prior written consent to the sub-Processing by Processor for purposes of Clause 11 of the Standard Contractual Clauses.

If the Processor intends to instruct sub-Processors other than the companies listed in Exhibit 2, the Processor will notify the Controller thereof in writing (email to the email address(es) on record in Processor's account information for Controller is sufficient) and will give the Controller the opportunity to object to the engagement of the new sub-Processors within 30 days after being notified. The objection must be based on reasonable grounds (e.g. if the Controller proves that significant risks for the protection of its Personal Data exist at the sub-Processor). If the Processor and Controller are unable to resolve such objection, either party may terminate the Terms and Conditions by providing written notice to the other party. Controller shall receive a refund of any prepaid but unused fees for the period following the effective date of termination.

Where Processor engages sub-Processors, Processor will enter into a contract with the sub-Processor that imposes on the sub-Processor the same obligations that apply to Processor under this ADC. Where the sub-Processor fails to fulfil its data protection obligations, Processor will remain liable to the Controller for the performance of such sub-Processors obligations.

Where a sub-Processor is engaged, the Controller must be granted the right to monitor and inspect the sub-Processor's activities in accordance with this ADC and the Data Protection Law, including to obtain information from the Processor, upon written request, on the substance of the contract and the implementation of the data protection obligations under the sub-Processing contract, where necessary by inspecting the relevant contract documents.

The provisions of this Section 4.6 shall mutually apply if the Processor engages a sub-Processor in a country outside the European Economic Area ("EEA") not recognized by the European Commission as providing an adequate level of protection for personal data. If, in the performance of this ADC, Makerble transfers any Personal Data to a sub-processor located outside of the EEA, Makerble shall, in advance of any such transfer, ensure that a legal mechanism to achieve adequacy in respect of that processing is in place.

**g. Data Transfers.** Controller acknowledges and agrees that, in connection with the performance of the services under the Terms and Conditions, Personal Data will be transferred to Makerble. The Standard Contractual Clauses at Exhibit 1 will apply with respect to Personal Data that is transferred outside the EEA, either directly or via onward transfer, to any country not recognized by the European

Commission as providing an adequate level of protection for personal data (as described in the Data Protection Law).

**h. Deletion or Retrieval of Personal Data.** Other than to the extent required to comply with Data Protection Law, following termination or expiry of the Terms and Conditions, Processor will delete all Personal Data (including copies thereof) processed pursuant to this ADC. If Processor is unable to delete Personal Data for technical or other reasons, Processor will apply measures to ensure that Personal Data is blocked from any further Processing.

Controller shall, upon termination or expiration of the Terms and Conditions and by way of issuing an Instruction, stipulate, within a period of time set by Processor, the reasonable measures to return data or to delete stored data. Any additional cost arising in connection with the return or deletion of Personal Data after the termination or expiration of the Terms and Conditions shall be borne by Controller.

## **5. Audits**

Controller may, prior to the commencement of Processing, and at regular intervals thereafter, audit the technical and organizational measures taken by Processor.

Processor shall, upon Controller's written request and within a reasonable period of time, provide Controller with all information necessary for such audit, to the extent that such information is within Processor's control and Processor is not precluded from disclosing it by applicable law, a duty of confidentiality, or any other obligation owed to a third party.

## **6. General Provisions**

In case of any conflict, this ADC shall take precedence over the regulations of the Terms and Conditions. Where individual provisions of this ADC are invalid or unenforceable, the validity and enforceability of the other provisions of this ADC shall not be affected.

Upon the incorporation of this ADC into the Terms and Conditions, the parties indicated in Section 7 below (Parties to this ADC) are agreeing to the Standard Contractual Clauses (where and as applicable) and all appendixes attached thereto. In the event of any conflict or inconsistency between this ADC and the Standard Contractual Clauses in Exhibit 1, the Standard Contractual Clauses shall prevail.

Effective 25 May 2018 Makerble will process Personal Data in accordance with the GDPR requirements contained herein which are directly applicable to Makerble's provision of its service to organisations.

## **7. Parties to this ADC**

This ADC is an amendment to and forms part of the Terms and Conditions. Upon the incorporation of this ADC into the Terms and Conditions, the Controller and Makerble are each a party to the Terms and Conditions and are also each a party to this ADC.

The legal entity agreeing to this ADC as Controller represents that it is authorized to agree to and enter into this ADC for, and is agreeing to this ADC solely on behalf of, the Controller.

## **EXHIBIT 1**

Standard Contractual Clauses (Processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection,

The Organisation using Makerble (the "data exporter")

And

Makerble, Make Worldwide Limited, 83 Ducie Street, Manchester, M1 2LQ, England, United Kingdom (the “data importer”),

each a ‘party’; together ‘the parties’,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

### **Clause 1**

#### Definitions

For the purposes of the Clauses:

(a) ‘personal data’, ‘special categories of data’, ‘process/processing’, ‘controller’, ‘processor’, ‘data subject’ and ‘supervisory authority’ shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) ‘the data exporter’ means the controller who transfers the personal data;

(c) ‘the data importer’ means the processor who agrees to receive from the data exporter personal data intended for processing on their behalf after the transfer in accordance with their instructions and the terms of the Clauses and who is not subject to a third country’s system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) ‘the subprocessor’ means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with their instructions, the terms of the Clauses and the terms of the written subcontract;

(e) ‘the applicable data protection law’ means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) ‘technical and organisational security measures’ means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

### **Clause 2**

#### Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

### **Clause 3**

#### Third-party beneficiary clause

- The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
- The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result

of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

- The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
- The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

#### **Clause 4**

##### Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).



## **Clause 5**

### Obligations of the data importer

The data importer agrees and warrants:

- (a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
- (d) that it will promptly notify the data exporter about:
  - (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;
  - (ii) any accidental or unauthorised access; and
  - (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
- (e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- (f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
- (g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
- (h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;
- (i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;
- (j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

## **Clause 6**

### Liability

- The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.
- If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or their subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.
- The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.
- If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

### **Clause 7**

#### Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

- (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
- (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

### **Clause 8**

#### Cooperation with supervisory authorities

- The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
- The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
- The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

### **Clause 9**

#### Governing law

The Clauses shall be governed by English law.

### **Clause 10**

#### Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

### **Clause 11**

#### Subprocessing

- The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
- The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
- The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by English law.
- The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

### **Clause 12**

#### Obligation after the termination of personal data-processing services

- The parties agree that on the termination of the provision of data-processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
- The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

### **APPENDIX 1 to the Standard Contractual Clauses**

This Appendix forms part of the Clauses. The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

#### **A. Data exporter**

The data exporter is the Organisation using Makerble, as defined in the Makerble Terms and Conditions.

#### **B. Data importer**

The data importer is Makerble, a provider of impact tracking software.

#### **C. Data subjects**

Categories of data subjects set out under Section 2 of the Terms and Conditions with Data Processors to which the Clauses are attached.

#### **D. Categories of data**

Categories of personal data set out under Section 2 of the Terms and Conditions with Data Processors to which the Clauses are attached.

#### **E. Special categories of data (if appropriate)**

The parties do not anticipate the transfer of special categories of data.

#### **F. Processing operations**

The processing activities set out under Section 2 of the Terms and Conditions with Data Processors to which the Clauses are attached:

### **Appendix 2 to the Standard Contractual Clauses**

This Appendix forms part of the Clauses.

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Makerble currently observes the security practices described in this Appendix 2. Notwithstanding any provision to the contrary otherwise agreed to by data exporter, Makerble may modify or update these practices at its discretion provided that such modification and update does not result in a material degradation in the protection offered by these practices.

#### **a) Access Control**

##### **i) Preventing Unauthorized Product Access**

**Outsourced processing:** Makerble hosts its Service with outsourced cloud infrastructure providers. Additionally, Makerble maintains contractual relationships with vendors in order to provide the Service in accordance with our Agreement with Data Processors. Makerble relies on contractual agreements, privacy policies, and vendor compliance programs in order to protect data processed or stored by these vendors.

**Physical and environmental security:** Makerble hosts its product infrastructure with outsourced infrastructure providers (Amazon Web Services and Heroku) which use industry standard security.

**Authentication:** Makerble has a password policy for its service. Organisations who use Makerble via the user interface must authenticate before accessing non-public customer data.

**Authorization:** Customer data is stored in cloud-based storage systems accessible to Organisations via the Makerble user interface and the application programming interfaces. Organisations are not allowed direct access to the underlying application infrastructure. The authorization model in Makerble's platform is designed to ensure that only the appropriately assigned individuals can access

relevant features, views, and customization options. Authorization to data sets is performed through validating the user's permissions against the attributes associated with each data set.

**Application Programming Interface (API) access:** Public product APIs may be accessed using an API key or through Oauth authorization.

## ii) Limitations of Privilege & Authorization Requirements

**Product access:** A subset of the Makerble team have access to the platform and to customer data via a secure interface. The intent of providing access to a subset of the team is to provide effective customer support when you ask us to help you with a customer service problem, to troubleshoot potential problems, to detect and respond to security incidents and implement data security. Their access is purely for technical reasons and is not for the purpose of using or acting upon any of the customer data. Each member of the team with this level of clearance has signed confidentiality agreements which prevent inappropriate use of any data they access. The permission to access data can be revoked from any member of this subset of the team at any time. In the event that an organisation requires members of Makerble's data protection team to sign an additional confidentiality agreement, this can be arranged. We take confidentiality seriously and are happy to discuss this further.

### b) Transmission Control

In-transit: Makerble makes HTTPS encryption (also referred to as SSL or TLS) available on every one of its login interfaces. Makerble's HTTPS implementation uses industry standard algorithms and certificates.

### c) Input Control

Response and tracking: Makerble maintains a record of known security incidents that includes description, dates and times of relevant activities, and incident disposition. Suspected and confirmed security incidents are investigated by security, operations, or support personnel; and appropriate resolution steps are identified and documented. For any confirmed incidents, Makerble will take appropriate steps to minimize product and Customer damage or unauthorized disclosure.

Communication: If Makerble becomes aware of unlawful access to Customer data stored within its products, Makerble will: 1) notify the affected Customers of the incident; 2) provide a description of the steps Makerble is taking to resolve the incident; and 3) provide status updates to the Customer contact, as Makerble deems necessary. Notification(s) of incidents, if any, will be delivered to one or more of the Customer's contacts in a form Makerble selects, which may include via email or telephone.

### d) Availability Control

Infrastructure availability: The infrastructure providers use commercially reasonable efforts to ensure a minimum of 99% uptime. The providers maintain a minimum of N+1 redundancy to power and network services.

Fault tolerance: Backup and replication strategies are designed to ensure redundancy and fail-over protections during a significant processing failure. Customer data is backed up.

## EXHIBIT 2

List of Sub-Processors

Amazon Web Services.

Google.

Heroku

Mailgun

Mailchimp

Tawk.to

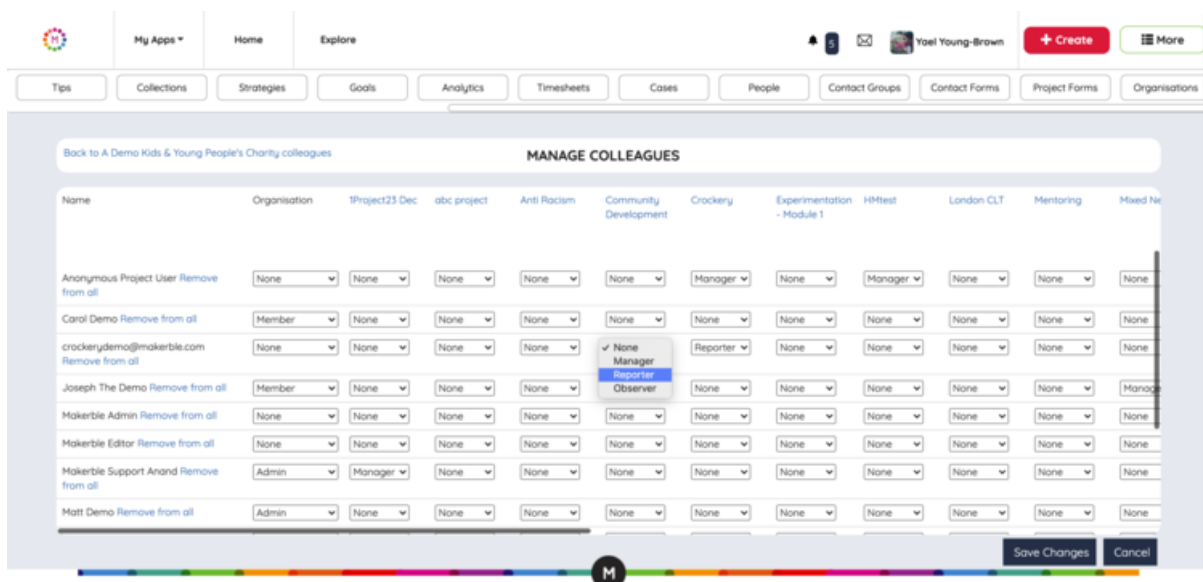
UserVoice

## Privacy by Design

We designed Makerble with privacy in mind from the outset. Every Makerble App has privacy controls woven into the user experience to give complete control over the level of access that each user has to every piece of data.

## Role-based User Access

Every organisation can manage its users from the Manage Colleagues page. Every user has an Organisation role and/or a Project role on every project they are part of.



The screenshot shows the 'MANAGE COLLEAGUES' page in a web application. The page has a navigation bar at the top with tabs for 'Tips', 'Collections', 'Strategies', 'Goals', 'Analytics', 'Timesheets', 'Cases', 'People', 'Contact Groups', 'Contact Forms', 'Project Forms', and 'Organisations'. Below the navigation bar is a table of users and their roles across various projects. The table has columns for 'Name', 'Organisation', and several project names. Each cell in the table contains a dropdown menu for selecting a role. The user 'crockerydemo@makerble.com' is highlighted, and a dropdown menu is open showing options: 'None', 'Manager', 'Reporter', and 'Observer'. The 'Reporter' option is selected. At the bottom right of the table, there are 'Save Changes' and 'Cancel' buttons.

Name	Organisation	Project23 Dec	abc project	Anti Racism	Community Development	Crockery	Experimentation - Module 1	HMtest	London CLT	Mentoring	Mixed Ne
Anonymous Project User Remove from all	None	None	None	None	None	Manager	None	Manager	None	None	None
Carol Demo Remove from all	Member	None	None	None	None	None	None	None	None	None	None
crockerydemo@makerble.com Remove from all	None	None	None	None	None	Reporter	None	None	None	None	None
Joseph The Demo Remove from all	Member	None	None	None	None	None	None	None	None	None	Manag
Makerble Admin Remove from all	None	None	None	None	None	None	None	None	None	None	None
Makerble Editor Remove from all	None	None	None	None	None	None	None	None	None	None	None
Makerble Support Anand Remove from all	Admin	Manager	None	None	None	None	None	None	None	None	None
Matt Demo Remove from all	Admin	None	None	None	None	None	None	None	None	None	None

## Roles:

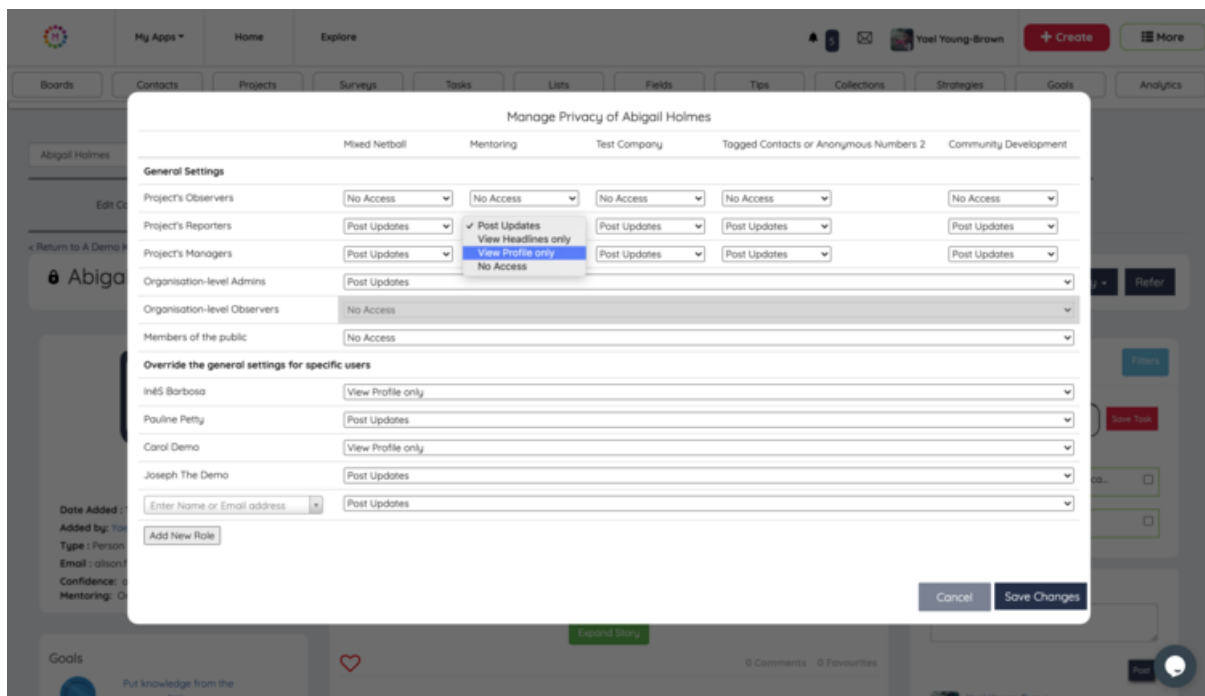
- **Organisation Roles:** Organisation Admin, Project Creator and Organisation Observer.
- **Project Roles:** Project Manager, Project Reporter and Project Observer.

## Examples:

- Frontline staff tend to be given the Project Reporter role on the specific projects that they are part of.
- Fundraising, Strategy, Operations and Reporting colleagues tend to be Project Observers so that they have Read Only access.

## Contact Privacy

Decide the level of access that each user has access to every contact in your database



### Access Levels to each individual Contact:

- **Post Update Access:** user is allowed to post updates, e.g. notes from a 1-2-1 meeting
- **Profile Access:** user is allowed to read-only access to the Contact record
- **Headline Access:** user is allowed to see the name of the Contact and other metadata such as the projects they are part of, but not the full Contact record
- **No Access:** user does not have any access to the Contact

Access Levels to each individual Contact are Role-based although you can make exceptions for specific users as required.

### Example:

- Mentors, Counsellors and Advisors typically have the Project Reporter role however because they are only meant to have access to the handful of people whom they support, the General Setting for Project Reporters in the Mentoring project would be No Access to this specific Contact but the Override Setting would be used to give the Mentor **Post Update Access** so that they can write up their session notes.

## Story Privacy

Every time you post an update about a project or contact, it is saved in your database as a story. Survey responses are saved as stories.

An Organisation Admin sets the default privacy level for all stories and decides whether the authors of each story are allowed to change the privacy settings of the stories they post.

## Progress Tracker Privacy

Assign particular outcomes, indicators, outputs and KPIs (Progress Trackers) to specific people. Determine whether other project colleagues have permission to see those Progress Trackers or not.

Project Team	(Test) Senzus Grown (Participation Tracker)	Boys Coached (Participation Tracker)	Children Coached (Participation Tracker)	Girls Coached (Participation Tracker)	Increased efficacy for reuse (Outcome Tracker)	Level of knowledge of reuse activities in the area (Achievement tickbox Tracker (Indicator))	Likelihood of engaging in reuse activities (Achievement tickbox Tracker (Indicator))	Test Scale 3 (Outcome Tracker)	Test Scale 3 (Multiple Choice Tracker (Indicator))
Visibility to other reporters	Private <input type="radio"/> Public <input checked="" type="radio"/>	Private <input type="radio"/> Public <input checked="" type="radio"/>	Private <input type="radio"/> Public <input checked="" type="radio"/>	Private <input type="radio"/> Public <input checked="" type="radio"/>	Private <input type="radio"/> Public <input checked="" type="radio"/>	Private <input type="radio"/> Public <input checked="" type="radio"/>	Private <input type="radio"/> Public <input checked="" type="radio"/>	Private <input type="radio"/> Public <input checked="" type="radio"/>	Private <input type="radio"/> Public <input checked="" type="radio"/>
Testing Angela	Assigned	Assigned	Assigned	Assigned	View Only	Assigned	Assigned	View Only	Assigned
Tim Test21	Assigned	Assigned	Assigned	Assigned	View Only	Assigned	Assigned	View Only	Assigned

## Progress Board Privacy

Progress Boards allow you to report your progress towards every outcome, indicator and metric you are tracking in your database. Choose whether you want funders, trustees or partners to have Read-only access to a particular Progress Board.

**Emotional Wellbeing**

Switch Board - Cards - Compare - Progress: Mine - All - Edit Board - New Board - Sort by - Filter Cards - My Cards Only

- Attendees**: across Lloyds Bank Foundation Gran... at A Demo Kids & Young People... (2027)
- children are more committed to sports**: across UK Projects of A Demo Kids & Young People... (2027)
- I rarely wake up feeling rested**: across UK Projects of A Demo Kids & Young People... (2027)
- Children joined**: across Lloyds Bank Foundation Gran... at A Demo Kids & Young People... (448)
- I feel that life is very rewarding**: across UK Projects of A Demo Kids & Young People... (2027)
- Sessions Held**: across Lloyds Bank Foundation Gran... at A Demo Kids & Young People... (2027)
- Activities done**: across Lloyds Bank Foundation Gran... at A Demo Kids & Young People... (310021)



### Project Privacy

Every area of work exists as its own project on Makerble. In addition to giving users Role-based Access to each project, Organisation Admins have the ability to set the privacy level of the project. This determines whether the project page is only visible to project colleagues (users who have been given Role-based Access to that project) or whether it is also visible on a Read-only basis to the wider set of Organisation Colleagues.

### Album Privacy

Albums pull together progress from multiple projects. A project can be part of many albums.

Album Privacy allows you to decide which users have access to that particular aggregated view of progress from multiple projects.