UK General Data Protection Policy
Provisional Compliance Document

Version 3.1 - 23 Nov 2022

1 Purpose & Introduction

This document is written in addition to the existing Sync Technologies Privacy Policy and will be in effect as of **15/12/2022** and is intended to demonstrate provisional compliance with the United Kingdom General Data Protection Regulation (UK GDPR) for any business conducted in the United Kingdom by Sync Technologies (Aust) Pty Ltd (ACN 644 357 273) of Tank Stream Labs, Level 7, 11 York Street, Sydney after **15/12/2022**.

Sync Technologies reserves the right to revise and update this document as needed to ensure compliance. If any such changes are made, any affected parties will be notified through a written notice. Revisions to any policies will be displayed in a notice on https://synctech.io indicating when any such revisions have been made.

This document was written in accordance with and in reference to the Guide to the General Data Protection Regulation (GDPR) by the Information Commissioner's Office (https://ico.org.uk).

This document was last updated on 23/11/23.

2 Definitions

For the purposes of this document, Sync Technologies references the definition of personal data, controllers and processors as defined by the Information Commissioner's Office (https://ico.org.uk):

> ***Personal data*** *includes information relating to natural persons who can be identified or who are identifiable, directly from the information in question; or can be indirectly identified from that information in combination with other information.*
>
> ***Controllers*** *mean 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.*
>
> ***Processors*** *mean the natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.*

Until further notice, for any business conducted in the United Kingdom, Sync Technologies will only act as a processor and only on behalf of other controllers.

3 Responsibilities

As a processor, Sync Technologies must uphold the principles as set out in Article 5(1) of the UK GDPR.

In addition, Sync Technologies must:

- Unless otherwise required by law, only process data on instructions from a controller.

- Enter into a binding contract with the controller in accordance with the requirements set out by the UK GDPR.
- Refrain from engaging sub-processors without prior specific or general written authorisation. If authorisation is given, Sync Technologies must put in place a contract with the sub-processor with terms that offer an equivalent level of protection for the personal data as those in the contract between Sync Technologies and the controller.
- Implement appropriate technical and organisational measures to ensure the security of personal data, including protection against accidental or unlawful destruction or loss, alteration, unauthorised disclosure or access.
- Notify the relevant controller in the event of a personal data breach without undue delay.
- Notify the relevant controller immediately if any of their instructions will lead to a breach of UK GDPR or local data protection laws.
- Comply with UK GDPR accountability obligations, such as maintaining records and appointing a data protection officer.
- Ensure that any transfer outside the UK is authorised by the controller and complies with the UK GDPR's transfer provisions.
- Cooperate with supervisory authorities (such as the ICO) to help them perform their duties.

4 Collection of Personal Data

Sync Technologies has identified the following personal data collected and stored by our products & services.

Personal Data	***Source***
User Full Name	Provided by controller.
User Mobile Number	Provided by controller.
User Email Address	Provided by controller.
Project Property Address	Provided by controller.
Client Reference Number	Provided by controller.
Claim Reference Number	Provided by controller, stored by subprocessor.
Project Property Site Contact Name	Provided by controller.
Project Property Site Contact Number	Provided by controller.
Project Property Site Contact Email	Provided by controller.
Project Property Virtual Tour	Processed by subprocessor and provided back to the controller.

In order to provide our products and services, Sync Technologies has identified the following subprocessors used to process and/or store personal data:

Subprocessor	Purpose	GDPR Compliant
ClickUp	Project Management	Yes
Make	Business Logic	Yes
Paperform	Booking Form	Yes
AWS	Database	Yes

5 Security & Encryption

Sync Technologies shall ensure that the following measures are taken with respect to the storage and disposal of personal data:

- Sync Technologies shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorized or unlawful processing and against accidental loss, destruction, or damage.
- All technical and organisational measures taken to protect personal data shall be regularly reviewed and evaluated to ensure their ongoing effectiveness and the continued security of personal data.
- Data security must be maintained at all times by protecting the confidentiality, integrity, and availability of all personal data as follows:
    a) only those with a genuine need to access and use personal data and who are authorised to do so may access and use it;
    b) personal data must be accurate and suitable for the purpose or purposes for which it is collected, held, and processed; and
    c) authorised users must always be able to access the personal data as required for the authorised purpose or purposes.

Data Security

Sync Technologies shall ensure that the following measures are taken with respect to the use of personal data:

- All electronic copies of personal data should be stored securely using passwords and data encryption.
- No hard copies of personal data will be stored.
- All personal data stored electronically will be backed up daily with backups stored for seven days. All backups will be encrypted.

- No personal data will be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to Sync Technologies or otherwise without the formal written approval of *Carolina Dreifuss (CEO)* at *carolina@synctech.io* and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than the accepted period as determined by the controller.

- No personal data should be transferred to any device personally belonging to an employee, agent, contractor, or other party working on behalf of Sync Technologies. Personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of Sync Technologies where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the applicable Data Protection Law.

- When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of.

- No personal data may be shared informally and if an employee, agent, contractor, or other party working on behalf of Sync Technologies requires access to any personal data that they do not already have access to, such access should be formally requested from the controller and Sync Technologies CEO, Carolina Dreifuss (carolina@synctech.io).

- No personal data may be transferred to any employee, agent, contractor, or other party, whether such parties are working on behalf of Sync Technologies or not, without the written authorisation of the controller and Sync Technologies CEO, Carolina Dreifuss (carolina@synctech.io).

- Personal data must be handled with care at all times and should not be left unattended or on view to unauthorized employees, agents, contractors, or other parties at any time.

- If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it.

Data Security - IT & Information Security

Sync Technologies shall ensure that the following measures are taken with respect to IT and information security:

- All passwords used to protect personal data must be changed regularly and must not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols. All passwords must be of a minimum of eight (8) characters and passwords must be changed every 60 days and must not be any of the 12 passwords used previously.

- Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of Sync Technologies, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords.

- All software (including, but not limited to, applications and operating systems) shall be kept up-to-date. Sync Technologies's IT staff shall be responsible for installing any and all security-related updates.

- No software may be installed on any Company-owned computer or device without the prior written approval of the IT Department

- All personal data, documents and sensitive information on the SyncTech platform, are password protected and encrypted and must not be transferred to any physical devices such as USBs, CDs and similar.

Organisational Measures

Sync Technologies shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

- All employees, agents, contractors, or other parties working on behalf Sync Technologies shall be made fully aware of both their individual responsibilities and Sync Technologies's responsibilities under Data Protection Law and under this Policy, and shall be provided with a copy of this Policy;
- Only employees, agents, contractors, or other parties working on behalf of Sync Technologies that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by Sync Technologies;
- All sharing of personal data shall comply with the information provided to the relevant data subjects and, if required, the consent of such data subjects shall be obtained prior to the sharing of their personal data.
- All employees, agents, contractors, or other parties working on behalf of Sync Technologies handling personal data will be appropriately trained to do so;
- All employees, agents, contractors, or other parties working on behalf of Sync Technologies handling personal data will be appropriately supervised;
- All employees, agents, contractors, or other parties working on behalf of Sync Technologies handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;
- All personal data held by Sync Technologies shall be reviewed periodically
- The performance of those employees, agents, contractors, or other parties working on behalf of Sync Technologies handling personal data shall be regularly evaluated and reviewed;
- All employees, agents, contractors, or other parties working on behalf of Sync Technologies handling personal data will be bound to do so in accordance with the principles of Data Protection Law and this Policy by contract;
- All agents, contractors, or other parties working on behalf of Sync Technologies handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and Data Protection Law;
- Where any agent, contractor or other party working on behalf of Sync Technologies handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless Sync Technologies against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure

6 Individual Rights

The Data Protection Principles

The UK GDPR sets out the following principles with which any party handling personal data must comply. Data controllers are responsible for and must be able to demonstrate such compliance. As a processor, Sync Technologies shall endeavour to uphold the principles as set out in the UK GDPR and all personal data must be:

- processed lawfully, fairly, and in a transparent manner in relation to the data subject;
- collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- adequate, relevant, and limited to what is necessary for relation to the purposes for which it is processed;
- accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay;
- kept in a manner that permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to the implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of the data subject;
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

The UK GDPR sets out the following key rights applicable to data subjects:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure (also known as the „right to be forgotten‟);
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- rights with respect to automated decision-making and profiling.

Lawful, Fair, and Transparent Data Processing

Data Protection Law seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. Specifically, the processing of personal data shall be lawful if at least one of the following applies:

- the data subject has given consent to the processing of their personal data for one or more specific purposes;
- the processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract;
- the processing is necessary for compliance with a legal obligation to which the data controller is subject;
- the processing is necessary to protect the vital interests of the data subject or of another natural person;
- the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or
- processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Consent

If consent is relied upon as the lawful basis for collecting, holding, and/or processing personal data, the following shall apply:

- Consent is a clear indication by the data subject that they agree to the processing of their personal data. Such a clear indication may take the form of a statement or a positive action. Silence, pre-ticked boxes, or inactivity are unlikely to amount to consent.
- Where consent is given in a document that includes other matters, the section dealing with consent must be kept clearly separate from such other matters.
- Data subjects are free to withdraw consent at any time and it must be made easy for them to do so. If a data subject withdraws consent, their request must be honoured promptly.
- If personal data is to be processed for a different purpose that is incompatible with the purpose or purposes for which that personal data was originally collected that was not disclosed to the data subject when they first provided their consent, consent to the new purpose or purposes may need to be obtained from the data subject.
- In all cases where consent is relied upon as the lawful basis for collecting, holding, and/or processing personal data, records must be kept of all consents obtained in order to ensure that Sync Technologies can demonstrate its compliance with consent requirements.

Specified, Explicit, and Legitimate Purposes

Sync Technologies collects and processes the personal data set out in Part 4 of this Policy. This includes:

- personal data collected directly from data subjects and
- personal data obtained from the data controller

Sync Technologies only collects, processes, and holds personal data for the specific purposes set out in Part 3 of this Policy (or for other purposes expressly permitted by Data Protection Law).

Adequate, Relevant, and Limited Data Processing

Sync Technologies will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed by the data controller as under Part 3 above, and as set out in Part 4.

- Employees, agents, contractors, or other parties working on behalf of Sync Technologies may collect personal data only to the extent required for the performance of their job duties and only in accordance with this Policy. Excessive personal data must not be collected.

- Employees, agents, contractors, or other parties working on behalf of Sync Technologies may process personal data only when the performance of their job duties requires it. Personal data held by Sync Technologies cannot be processed for any unrelated reasons.

Accuracy of Data and Keeping Data Up-to-Date

Sync Technologies shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out in “Rectification of Personal Data” below.

The accuracy of personal data shall be checked when it is collected and. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

Data Retention

Sync Technologies shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed. When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

.

Accountability and Record-Keeping

Sync Technologies shall follow a privacy-by-design approach at all times when collecting, holding, and processing personal data. Data Protection Impact Assessments shall be conducted if any processing presents a significant risk to the rights and freedoms of data subjects.

- All employees, agents, contractors, or other parties working on behalf of Sync Technologies shall be given appropriate training in data protection and privacy, addressing the relevant aspects of the Data Protection Law, this Policy, and all other applicable Company policies.

- Sync Technologies’s data protection compliance shall be regularly reviewed and evaluated by means of Data Protection Audits.

- Sync Technologies shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

a) the name and details of Sync Technologies, its Data Protection Officer, and any applicable third-party data transfers (including data processors and other data controllers with whom personal data is shared);
b) the purposes for which Sync Technologies collects holds, and processes personal data;
c) details of the categories of personal data collected, held and processed by Sync Technologies, and the categories of data subject to which that personal data relates;
d) details of how long personal data will be retained by Sync Technologies
e) details of personal data storage, including location(s);
f) detailed descriptions of all technical and organisational measures taken by Sync Technologies to ensure the security of personal data

Data Protection Impact Assessments and Privacy by Design

In accordance with the privacy by design principles, Sync Technologies shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data which involve the use of new technologies and where the processing involved is likely to result in a high risk to the rights and freedoms of data subjects.

- The principles of privacy by design should be followed at all times when collecting, holding, and processing personal data. The following factors should be taken into consideration:
    a) the nature, scope, context, and purpose or purposes of the collection, holding, and processing;
    b) the state of the art of all relevant technical and organisational measures to be taken;
    c) the cost of implementing such measures; and
    d) the risks posed to data subjects, and to Sync Technologies, including their likelihood and severity.

- Data Protection Impact Assessments shall be overseen by the Data Protection Officer and shall address the following:
    a) the type(s) of personal data that will be collected, held, and processed;
    b) the purpose(s) for which personal data is to be used;
    c) Sync Technologies‘s objectives;
    d) how personal data is to be used;
    e) the parties (internal and/or external) who are to be consulted;
    f) the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;
    g) risks posed to data subjects;
    h) risks posed both within and to the Sync Technologies; and
    i) proposed measures to minimise and handle identified risks.

Keeping Data Subjects Informed

Sync Technologies shall provide the information to every data subject:

a) where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and
b) where personal data is obtained from the data controller, the relevant data subjects will be informed of its purpose:
    i) if the personal data is used to communicate with the data subject, when the first communication is made; or

ii) if the personal data is to be transferred to another party, before that transfer is made; or

iii) as soon as reasonably possible and in any event, not more than one month after the personal data is obtained.

The following information shall be provided in the form of a privacy notice:

a) details of Sync Technologies including, but not limited to, contact details, and the names and contact details of any applicable representatives and its Data Protection Officer;
b) the purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 3 and 4 of this Policy
c) where applicable, the legitimate interests upon which Sync Technologies is justifying its collection and processing of the personal data;
d) where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;
e) where the personal data is to be transferred to one or more third parties, details of those parties;
f) details of applicable data retention periods;
g) details of the data subject‟s rights under the UK GDPR;
h) details of the data subject‟s right to withdraw their consent to Sync Technologies's processing of their personal data at any time;
i) details of the data subject's right to complain to the Information Commissioner's Office;
j) where the personal data is not obtained directly from the data subject, details about the source of that personal data;
k) where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and
l) details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences

Data Subject Access

Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data that Sync Technologies holds about them, what it is doing with that personal data, and why.

- Employees wishing to make a SAR should do so using a Subject Access Request Form, sending the form to Sync Technologies's Data Protection Officer.

- Responses to SARs must normally be made within one month of receipt, however, this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

- All SARs received shall be handled by Sync Technologies's Data Protection Officer.

- Sync Technologies does not charge a fee for the handling of normal SARs. Sync Technologies reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

Rectification of Personal Data

Data subjects have the right to require Sync Technologies to rectify any of their personal data that is inaccurate or incomplete.

- Sync Technologies shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing Sync Technologies of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

- In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

Erasure of Personal Data

Data subjects have the right to request Sync Technologies erases the personal data it holds about them in the following circumstances:

a) it is no longer necessary for Sync Technologies to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;
b) the data subject wishes to withdraw their consent to Sync Technologies holding and processing their personal data;
c) the data subject objects to Sync Technologies holding and processing their personal data;
d) the personal data has been processed unlawfully;
e) the personal data needs to be erased in order for Sync Technologies to comply with a particular legal obligation;
f) personal data is being held and processed for the purpose of providing information society services to a child.

Unless Sync Technologies has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject‟s request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

In the event that any personal data that is to be erased in response to a data subject‟s request has been disclosed to third parties, those parties shall be informed of the erasure unless it is impossible or would require disproportionate effort.

Restriction of Personal Data Processing

Data subjects may request that Sync Technologies ceases processing the personal data it holds about them. If a data subject makes such a request, Sync Technologies shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.

In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

Objections to Personal Data Processing

Data subjects have the right to object to Sync Technologies processing their personal data.

- Where a data subject objects to Sync Technologies processing their personal data based on its legitimate interests, Sync Technologies shall cease such processing immediately, unless it can be demonstrated that Sync Technologies's legitimate grounds for such processing override the data subject‟s interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

- Where a data subject objects to Sync Technologies processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under the UK GDPR, demonstrate grounds relating to his or her particular situation. Sync Technologies is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

7 Transferring Personal Data to a Country Outside the UK

Sync Technologies may, from time to time, transfer ("transfer‟ includes making available remotely) personal data to countries outside of the UK. The UK GDPR restricts such transfers in order to ensure that the level of protection given to data subjects is not compromised.

Personal data may only be transferred to a country outside the UK if one of the following applies:

a) The UK has issued regulations confirming that the country in question ensures an adequate level of protection (referred to as "adequacy decisions‟ or "adequacy regulations‟). From 1 January 2021, transfers of personal data from the UK to EEA countries will continue to be permitted. Transitional provisions are also in place to recognise pre existing EU adequacy decisions in the UK.
b) Appropriate safeguards are in place including binding corporate rules, standard contractual clauses approved for use in the UK (this includes those adopted by the European Commission prior to 1 January 2021), an approved code of conduct, or an approved certification mechanism.
c) The transfer is made with the informed and explicit consent of the relevant data subject(s).
d) The transfer is necessary for one of the other reasons set out in the UK GDPR including the performance of a contract between the data subject and the Company; public interest reasons; for the establishment, exercise, or defence of legal claims; to protect the vital interests of the data subject where the data subject is physically or legally incapable of giving consent; or, in limited circumstances, for the Company's legitimate interests.

8 Data Breaches

All personal data breaches must be reported immediately to Sync Technologies's Data Protection Officer and Carolina Dreifuss (CEO) at carolina@synctech.io.

- If an employee, agent, contractor, or other party working on behalf of Sync Technologies becomes aware of or suspects that a personal data breach has occurred, they must not attempt to investigate it themselves. Any and all evidence relating to the personal data breach in question should be carefully retained.

    - If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage),

the Data Protection Officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

- In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described above) to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay

- In the event of a personal data breach, any and all affected controllers shall be notified within 24 hours after Sync Technologies has been made aware of such a breach.

- Data breach notifications shall include the following information:

    a) The categories and approximate number of data subjects concerned;
    b) The categories and approximate number of personal data records concerned;
    c) The name and contact details of Sync Technologies's data protection officer (or other contact points where more information can be obtained);
    d) The likely consequences of the breach;
    e) Details of the measures taken, or proposed to be taken, by Sync Technologies to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

Implementation of Policy

This Policy shall be deemed effective as of **15/12/2022**. No part of this Policy shall have a retroactive effect and shall thus apply only to matters occurring on or after this date for all business purposes conducted within the United Kingdom.

This Policy has been approved and authorised by:

Name: Carolina Dreifuss Aravena
Position: CEO
Date: 23 Nov 2022
Due for Review by: 1 March 2023

Signature: