Data Processing Addendum
to the Tracking Time, LLC Terms of Service

This Addendum ("**Addendum**") supplements and amends the TrackingTime, LLC Terms of Service (the "**Agreement**") agreed between:

1. **Tracking Time, LLC**, a Delaware corporation, with principal offices located at 1000 E Hallandale Beach Blvd, Suite 28, Hallandale Beach, FL33009 ("**TrackingTime**"); and
2. The customer identified in the signature block below ("**Customer**"). This Addendum is dated as of the date when it is signed by both parties.

BACKGROUND

The Agreement governs the supply by TrackingTime of cloud-based time tracking software services wherein time entries and other data uploaded by the Customer or its employees and contractors are stored by TrackingTime. This Addendum sets out the terms of the Agreement governing data processing.

AGREED TERMS

1. Definitions

1.1. Except as expressly stated in this section 1, words and phrases defined in the Agreement have the same meaning in this Addendum.

1.2. "**Compliant Jurisdiction**" means (i) the United Kingdom, or (ii) a country within the European Economic Area, or (iii) a country with the benefit of a favorable adequacy decision under Article 45 of Regulation (EU) 2016/679.

1.3. "**EU Data Protection Legislation**" means Regulation (EU) 2016/679 (commonly known as the General Data Protection Regulation) as amended from time to time.

1.4. References to '**Controller**', '**Data Subject**, '**Personal Data**', '**Data Breach**', '**Processor**', '**Processing**' and '**Supervisory Authority**' have the meanings defined in the EU Data Protection Legislation. References to '**Sub-Processor**' mean another processor appointed by a processor.

2. Status of this Addendum

2.1. This Addendum supplements the terms of the Agreement. It forms part of the Agreement.

2.2. This Addendum applies only to Customer Data that includes (or might potentially include) Personal Data in circumstances where the Processing of that Personal Data is subject to EU Data Protection Legislation.

2.3. If this Addendum is inconsistent with any other provisions of the Agreement, the parties intend that the provisions of this Addendum should prevail.

3. EU Data Protection Legislation

3.1. For all Personal Data provided to TrackingTime by or on behalf of Customer for Processing under the Agreement, the parties intend that Customer is the Controller and TrackingTime is the Processor of the Personal Data.

3.2. Except for (i) login details of Service Users; and (ii) Customer Data that happens to include Personal Data and is supplied to TrackingTime personnel by Customer otherwise than by uploading it as Customer Data to the Services (there being no

obligation or expectation of such supply), TrackingTime represents and Customer agrees as follows:

3.2.1. TrackingTime does not:

3.2.1.1. ascertain whether Customer Data includes Personal Data (and TrackingTime therefore treats all Customer Data as if it might include Personal Data);

3.2.1.2. ascertain whether Customer Data includes any special categories of Personal Data (and TrackingTime will not treat any such Customer Data any differently if Customer uploads such data to the Services contrary to the prohibition on doing so contained herein);

3.2.1.3. ascertain whether Customer Data includes any personal data concerning children;

3.2.1.4. ascertain whether the Services are used by Service Users to process outside the European Economic Area;

3.2.1.5. keep a record of Processing with any greater information than that which is required to be kept by TrackingTime pursuant the Agreement and this Addendum.

4. Protection of Personal Data

If the Customer uses the Services to Process any Customer Data that includes Personal Data in circumstances where the Processing of that Personal Data is subject to EU Data Protection Legislation, for the purpose of ensuring adequate protection as required by Article 45 of GDPR TrackingTime shall, upon request by Customer, execute in favor of the Customer the Standard Contractual Clauses substantially in the form set out in Exhibit 1 to this Addendum.

Notwithstanding Claus 4(g) of the Contractual Clauses the parties hereby expressly agree that the Customer shall not use the Services to process any special categories of Personal Data, including Sensitive Data as defined in EU Data Protection Legislation.

[REMAINDER OF PAGE INTENTIONALLY BLANK]

Signed for and on behalf of
Tracking Time, LLC.

By: DocuSigned by: Diego Wyllie 30ECFDBEC2E6474...

Name: Diego Wyllie

Title: Co-founder

Dated: 6/1/2018 7:10:50 AM PDT

Signed for and on behalf of
[Customer's Legal Name]

[Customer's Registered or Principal Place of Business Address]

[Name of Customer's Data Protection Officer (if applicable)]

By: _____

Name: _____

Title: _____

Dated: _____

EXHIBIT 1: STANDARD CONTRACTUAL CLAUSES

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 gaps below are populated with details of the relevant Company Group Member:*]

Name of the data exporting organization (customer's name):

Address:

Tel.:_____; fax:_____; e-mail: _____

Other information needed to identify the organization

……
(the data **exporter**)

and

Name of the data importing organization: **Tracking Time, LLC**

Address: 1000 E HALLANDALE BEACH BLVD STE 28. Hallandale Beach. 33009 Florida

Tel.: +1 (585) 457-5087

e-mail: support@trackingtime.co

Other information needed to identify the organization:

Tracking Time, LLC is a Delaware limited liability company

(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.

Background

The data exporter has entered into a data processing addendum ("DPA") with the data importer. Pursuant to the terms of the DPA, it is contemplated that services provided by the data importer will involve the transfer of personal data to data importer. Data importer is located in a country not ensuring an adequate level of data protection. To ensure compliance with Directive 95/46/EC and applicable data protection law, the controller agrees to the provision of such Services, including the processing of

personal data incidental thereto, subject to the data importer's execution of, and compliance with, the terms of these Clauses.

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 his behalf after the transfer in accordance with his 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 his 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

1. 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.

2. 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.

3. 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.

4. 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 organizational 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, unauthorized 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 organizational 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 unauthorized access, and

  (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorized 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

1. 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.

2. 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 his 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 of 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.

3. 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

1. 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.
2. 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.
3. 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 the law of the Member State in which the data exporter is established.

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

1. 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.
2. 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.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. 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

1. 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.
2. 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.

On behalf of the data exporter:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature…….

On behalf of the data importer:

Name (written out in full): Diego Wyllie

Position: CTO

Address: 1000 E Hallandale Blvd, Suite 28, Hallandale Beach, FL 33009

Other information necessary in order for the contract to be binding (if any):

Signature…… DocuSigned by: Diego Wyllie 30ECFDBEC2E6474...

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter
The data exporter is the party named on the signature page hereto.

Data importer
The data importer is
Tracking Time, LLC

Data subjects
The personal data transferred concern the following categories of data subjects: employees or contractors of the Data Exporter; other persons named or identified by the employees or contractors of the data exporter in connection with their use of the Services.

Categories of data
The personal data transferred concern the following categories of data:

- TrackingTime maintains Log-in credentials for Service Users as created by the Data Exporter or Service User.
- Additional types and categories of Personal Data and Data Subjects which the Customer may process within the Services are as follows:
    - Time entries (date, start time, end time, user, task, notes)
    - Tasks and Subtasks, Task Lists and Task Comments
    - Projects
    - Customers
    - Services
    - Work schedules
    - Users (given name, family name, email address, password (encrypted), role, status, employer organization, details of use of the Services).
    - Miscellaneous Personal Data entered by a user in connection with their use of the Services (for example, naming a third party in a time entry). The Data Importer does not seek to identify this type of personal data.

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data: none.

Processing operations
The personal data transferred will be subject to the following basic processing activities:

- TrackingTime verifies that only credentials authorized by the Customer are authenticated for access to the Services
- Storing, indexing, retrieving, searching and distributing time entries and associated information generated in the course of the Data Exporter's business for the purpose of providing the Data Exporter with a time tracking system
- Encrypting data in transit and decrypting the data to render underlying files in their original machine and human readable format upon the instructions of Service users

Sub-processors
The data importer has subcontracted some processing of personal data as follows:

Entity Name	**Entity Type**	**Entity Country**
Mixpanel	Product Analytics	United States
Google Analytics	Web Analytics	United States
Intercom	Customer Messaging	Ireland
Amazon Web Services	Cloud Infrastructure Services	United States
Nubity	DevOps Management	United States
CloudFlare	Content Delivery Network	United States
MailChimp	Email messaging	United States
Stripe	Payments Provider	United States
Baremetrics	Business Analytics	United States

DATA EXPORTER

Name:……

Authorized Signature ……

DATA IMPORTER

Tracking Time, LLC

Name: Diego Wyllie

Authorized Signature …… DocuSigned by: Diego Wyllie 30ECFDBEC2E6474...

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

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

In this Appendix 2:

"Agreement" means the TrackingTime Terms of Service between Customer and TrackingTime.
"Customer" means the data exporter.
"TrackingTime" means the data importer.

1. Except for (i) login details of Service Users; and (ii) Customer data that happens to include personal data and is supplied to TrackingTime personnel by Customer otherwise than by uploading it as Customer data to the Services (there being no obligation or expectation of such supply), TrackingTime represents and Customer agrees as follows:

    1. TrackingTime does not:

    1.1. ascertain whether Customer Data includes Personal Data (and TrackingTime therefore treats all Customer Data as if it might include Personal Data);

    1.2. ascertain whether Customer Data includes any special categories of Personal Data (and TrackingTime will not treat any such Customer Data any differently if Customer uploads such data to the Services contrary to the prohibition on doing so contained herein);

    1.3. ascertain whether Customer Data includes any personal data concerning children;

    1.4. ascertain whether the Services are used by Service Users to process outside the European Economic Area;

    1.5. keep a record of Processing with any greater information than that which is required to be kept by TrackingTime pursuant the Agreement and this Addendum.

2. TrackingTime further agrees to:

    2.1. if there is a personal data breach in relation to any Customer data, notify the Customer without undue delay and, where practicable, within 48 hours and thereafter assist the Customer with its obligations to notify the personal data breach to a supervisory authority;

    2.2. provide the Customer with reasonable assistance to undertake data protection impact assessments in relation to processing of personal data pursuant to the Agreement and reasonable assistance requested by Customer in relation to any consultation with a supervisory authority that the Customer carries out in relation to such assessment, provided Customer bears the cost of TrackingTime preparing data protection impact assessments for the Customer or providing reasonable assistance in consultation with a supervisory authority; and

    2.3. make available to the Customer its standard Due Diligence Response (DDR) package which contains all information necessary to demonstrate compliance with the obligations in the Agreement and the Standard Contractual Clauses. Additionally, TrackingTime will allow for and contribute to audits, including inspections, conducted by the Customer or another auditor mandated by the Customer, provided Customer bears the cost of the audit and auditors

3. To the extent that TrackingTime uses another processor to process any Customer data,

it is agreed that:

3.1. the Sub-Processors at the date of these Standard Contractual Clauses are as set out in Appendix 1;

3.2. the Services and such sub-processor are common to all TrackingTime customers;

3.3. TrackingTime is responsible for the acts and omissions of its sub-processors;

3.4. from time to time and in its sole discretion, TrackingTime may appoint different sub-processors;

3.5. TrackingTime shall notify the Customer in advance of any changed or new sub-processors or any material change to the processing done by sub-processors, thereby giving the Customer an opportunity to object to such changes;

3.6. TrackingTime shall ensure that each sub-processor agrees to contractual obligations and restrictions consistent with the provisions of the Standard Contractual Clauses;

and the parties agree that:

3.7. if TrackingTime notifies the Customer of any changes to sub-processors and the Customer objects to such changes, the Customer will be entitled to terminate the Agreement (without liability for either party, and such termination will be deemed to be a no-fault termination) if the Customer has reasonable grounds for objecting to such changes on the grounds that the changes would cause the Customer to be in breach of EU Data Protection Legislation.

The measures deployed at any one time by TrackingTime are set out at Appendix 3–TrackingTime Security Summary. Without limiting TrackingTime' obligations in the Standard Contractual Clauses, TrackingTime may change the measures so that they adapt to reflect changes in the Services and the state of the art as regards information security.

APPENDIX 3 TO THE STANDARD CONTRACTUAL CLAUSES

TrackingTime Security Summary

TrackingTime employs a comprehensive range of procedures, tools, and independent services to provide industry-leading security for information processed through its Services. Below is a summary overview of many of the security features used by TrackingTime as of the date of this Addendum:

- TrackingTime's cloud-based application is hosted on Amazon Web Services (AWS), which is certified for the EU-US privacy shield. Amazon provides power, hardware, network and the highest on-site security standards for data centers.
- TrackingTime’s underlying infrastructure for our cloud application is only accessible via an encrypted SSL connection.
- TrackingTime’s servers are protected behind state-of-the-art firewall technology.
- All TrackingTime customer data is backed-up on a daily basis.
- The TrackingTime cloud platform is built on top of enterprise-class Java technologies, the same used by the most prestigious e-commerce platforms and online banks around the world.
- The TrackingTime frontend application itself runs on a separate hardware node than that on which the data is securely stored.
- TrackingTime Customer data is physically protected in data center facilities managed by AWS engineers and safeguarded by redundant systems.
- Application database backups for TrackingTime are performed daily and retained for 14 days.
- All communications between client applications (i.e. the web, desktop and mobile TrackingTime apps used by our customers) and the backend servers are encrypted using SSL and protected by a robust firewall system designed by security experts at the Apache Software Foundation.
- User passwords are cryptographically hashed using state-of-the-art algorithms (SHA-256).
- All payments are securely processed by Stripe, our payments provider, in accordance with PCI Data Security Standards. Credit card details are never directly processed by us nor stored on our servers.