# Data Processing Addendum

This Data Processing Addendum (**Addendum**) forms part of the TrafficGuard Terms of Service (available at https://trafficguard.ai/terms) (or where applicable Pricing Plan Agreement) ( **Service Agreement**) between: (i) TrafficGuard Pty Ltd., Suite 10, 16 Brodie Hall Drive, Technology Park, WA 6102 Bentley, Australia (**TrafficGuard** ) and (ii) and the Customer who agreed to and is party to the Service Agreement (**Customer**).

The terms used in this Addendum shall have the meanings set forth in this Addendum. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Service Agreement Except as modified below, the terms of the Service Agreement shall remain in full force and effect .

In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Service Agreement. Except where the context requires otherwise, references in this Addendum to the Service Agreement are to the Service Agreement as amended by, and including, this Addendum.

## 1. Definitions

1.1. In this Addendum, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

1.1.1. **CCPA** means the California Consumer Privacy Act, Cal. Civ. Code 1798.100 et seq., including any amendments and any implementing regulations thereto that become effective on or after the effective date of this Addendum;

1.1.2. **Customer Personal Data** means any Personal Data Processed by TrafficGuard (or a Subprocessor) on behalf of Customer pursuant to or in connection with the Service Agreement;

1.1.3. **EEA** means the European Economic Area;

1.1.4. **EU** means the European Union;

1.1.5. **Data Protection Laws** means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, including the GDPR (as defined below) and laws implementing or supplementing the GDPR;

1.1.6. **GDPR** means the EU General Data Protection Regulation 2016/679;

1.1.7. **Services** means the services and other activities to be supplied to or carried out by or on behalf of TrafficGuard for Customer pursuant to the Service Agreement;

1.1.8. **Standard Contractual Clauses** means the contractual clauses set out in Appendix 3 and under section 10;

1.1.9. **Subprocessor** means any person appointed by or on behalf of TrafficGuard to Process Personal Data on behalf of Customer in connection with the Service Agreement; and

1.1.10. **TrafficGuard Affiliate** means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with TrafficGuard, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.

1.2. The terms, **Commission**, **Controller**, **Data Protection Officer**, **Data Subject**, **Member State**, **Personal Data**, **Personal Data Breach**, **Processing**, **Representative** and **Supervisory Authority** shall have the same meaning as in the GDPR, and their related terms shall be construed accordingly.

1.3. The word **include** shall be construed to mean include without limitation, and related terms shall be construed accordingly.

1.4. **Privacy Policy** means the policy available at https://trafficguard.ai/privacy-policy

# 2. Processing of Personal Data

## 2.1. TrafficGuard

2.1.1. will Process Customer Personal Data in accordance with those Data Protection Laws, including GDPR requirements where relevant, directly applicable to TrafficGuard's provision of the Services; and

2.1.2. shall only Process Customer Personal Data on behalf of and in accordance with Customer's documented instructions.

## 2.2. Customer

2.2.1. represents, warrants and covenants that it has provided notice to its users that it shares Personal information (as defined in the CCPA) with Service Providers (as defined in the CCPA) for the purpose of providing services to users;

2.2.2. agrees that TrafficGuard is a "Service Provider," as that term is defined in Section 1798.140(v) of the CCPA;

2.2.3. agrees that it is necessary for to maintain Personal Information in order to detect security incidents, or protect against malicious, deceptive, fraudulent, or illegal activity pursuant to Section 1798.105(d)(2) of the CCPA;

2.2.4. shall, in its use or receipt of the Services, Process Customer Personal Data in accordance with the requirements of Data Protection Laws and Customer will ensure that its instructions for the Processing of Customer Personal Data shall comply with Data Protection Laws. Customer shall have sole responsibility for the accuracy, quality, and legality of Customer Personal Data and the means by which Customer acquired such Personal Data; and

2.2.5. instructs TrafficGuard to

2.2.5.1. Process Customer Personal Data; and in particular, transfer Customer Personal Data to any country or territory, in both cases as reasonably necessary for the provision of the Services and consistent with the Service Agreement.

2.2.6. Appendix 1 to this Addendum sets out certain information regarding the Processing of the Customer Personal Data as required by Article 28(3) of the GDPR. Upon prior written notice, Customer may request reasonable amendments to Appendix 1 as Customer reasonably considers necessary to meet those requirements.

## 3. Personnel, Quality assurance and other duties of TrafficGuard

3.1. TrafficGuard shall ensure that its personnel engaged in the Processing of Customer Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and are subject to obligations of confidentiality and such obligations survive the termination of that person's' engagement with TrafficGuard.

3.2. TrafficGuard shall take commercially reasonable steps to ensure the reliability of any TrafficGuard personnel engaged in the Processing of Customer Personal Data.

3.3. TrafficGuard shall ensure that access to Personal Data is limited to those personnel who require such access to perform the Service Agreement.

3.4. TrafficGuard has appointed a Data Protection Officer. The individual appointed may be reached at the contact details specified in the Privacy Policy.

3.5. As TrafficGuard is established outside the EU/EEA, it has designated a Representative within the European Union pursuant to Article 27(1) of the GDPR. The contact details of the Representative are specified in the Privacy Policy.

## 4. Security

4.1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Customer and TrafficGuard shall implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

4.2. TrafficGuard will maintain appropriate technical and organizational measures for protection of the security, confidentiality and integrity of Customer Personal Data that meet the requirements for a Data Processor under the GDPR, as set forth in Appendix 2 to this Addendum. TrafficGuard regularly monitors compliance with these safeguards. TrafficGuard will not materially decrease the overall security of the

Services during the term of TrafficGuard's provision of such Services pursuant to the Service Agreement.

## 5. Subprocessors

5.1. Customer acknowledges and agrees that (a) TrafficGuard Affiliates may be retained as Subprocessors; and (b) TrafficGuard may engage third-party Subprocessors in connection with the provision of the Services. Any such Subprocessors will be permitted to obtain Customer Personal Data only for the purposes of providing the Services. TrafficGuard has retained them to provide, and they are prohibited from using Customer Personal Data for any other purpose.

5.2. TrafficGuard shall be liable for the acts and omissions of its Subprocessors to the same extent TrafficGuard would be liable if performing the Services of each Subprocessor directly under the terms of this Addendum, except as otherwise set forth in the Service Agreement.

5.3. TrafficGuard has entered into a written agreement with each Subprocessor containing data protection obligations that are at least as protective as the terms set forth in this Addendum with respect to the protection of Customer Personal Data and meet the requirements of Article 28(3) of the GDPR or equivalent provisions of any other Data Protection Law, to the extent applicable to the nature of the Services provided by such Subprocessor.

5.4. Customer authorises TrafficGuard to appoint Subprocessors in accordance with this section 5. The list of Subprocessors currently used by TrafficGuard in connection with its provision of the Services is set forth in Appendix 1, as well as those listed on TrafficGuard's website.

5.5. TrafficGuard shall give notice to Customer via TrafficGuard's website of the appointment of any new Subprocessor, including full details of the Processing to be undertaken by the Subprocessor (Customer is responsible for regularly checking and reviewing TrafficGuard's website for any such changes). If, within 30 business days of receipt of that notice, Customer notifies TrafficGuard in writing of any objections (on reasonable grounds) to the proposed appointment, TrafficGuard will take commercially reasonable steps to address the objections raised by Customer and provide Customer with reasonable written explanation of the steps taken to address such objection.

5.6. In the event that the Subprocessor provides the agreed service outside the EU/EEA, TrafficGuard shall ensure compliance with the Data Protection Laws, in particular the requirements of Articles 44 et seq. GDPR.

## 6. Rights of Data Subject

6.1. Taking into account the nature of the Processing, TrafficGuard shall assist Customer by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests to

exercise Data Subject rights under the Data Protection Laws, in particular under Chapter III of the GDPR ("Data Subject Request").

6.2. TrafficGuard shall, to the extent legally permitted, promptly notify Customer if it receives a Data Subject Request in respect of Customer Personal Data. TrafficGuard shall not respond to any such request except on the documented instructions of Customer.

6.3. Furthermore, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, TrafficGuard shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to a Data Subject Request, to the extent TrafficGuard is legally permitted to do so and provided that such Data Subject Request is required under the Data Protection Laws.

6.4. Any costs arising from the provision of assistance under this section 6 shall be the responsibility of Customer, to the extent legally permitted.

## 7. Personal Data Breach and Data Protection Impact Assessment

7.1. TrafficGuard shall notify Customer without undue delay should TrafficGuard become aware of a Personal Data Breach affecting Customer Personal Data, and shall provide Customer with sufficient information to allow Customer to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws. TrafficGuard shall cooperate with Customer and take such reasonable commercial steps as are directed by Customer to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

7.2. TrafficGuard shall provide Customer with reasonable assistance as needed to fulfil Customer's obligation to carry out a data protection impact assessment under Article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Customer Personal Data by, and taking into account the nature of the Processing and information available to TrafficGuard.

7.3. Any costs arising from the provision of assistance under this section 7 shall be the responsibility of Customer, to the extent legally permitted.

## 8. Deletion or return of Customer Personal Data

At Customer's request, except for that Personal Data with respect to which TrafficGuard acts as a Data Controller, TrafficGuard shall delete or return all Customer Personal Data to Customer after the end of the provision of Services relating to Processing, and delete existing copies, in accordance with the policies set out in the Privacy Policy, unless applicable Data Protection Law requires storage of the Personal Data.

## 9. Audit rights

9.1. Subject to sections 9.2 to 9.3, TrafficGuard shall make available to Customer on request all information necessary to demonstrate compliance with this Addendum, and shall allow for and contribute to audits, including inspections, by Customer or an auditor mandated by Customer in relation to the Processing of the Customer Personal Data by TrafficGuard.

9.2. Information and audit rights of Customer only arise under section 9.1 to the extent that the Service Agreement does not otherwise give the Customer information and audit rights meeting the relevant requirements of Data Protection Law (including, where applicable, point (h) of Article 28(3) GDPR).

9.3. Customer shall give TrafficGuard reasonable notice of any audit or inspection to be conducted under section 9.1 and shall take (and ensure that each of its mandated auditors takes) reasonable measures to avoid causing (or, if it cannot avoid, to minimise) any damage, injury or disruption to TrafficGuard's premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection. TrafficGuard need not give access to its premises for the purposes of such an audit or inspection:

9.3.1. to any individual unless he or she produces reasonable evidence of identity and authority;

9.3.2. outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and Customer has given notice to TrafficGuard that this is the case before attendance outside those hours begins; or

9.3.3. for the purposes of more than one audit or inspection in any calendar year, except for any additional audits or inspections where Customer is required or requested to carry out such under Data Protection Law or by a Supervisory Authority or any similar regulatory authority responsible for the enforcement of Data Protection Laws in any country or territory, and where Customer has identified the relevant requirement or request in its notice to TrafficGuard of the audit or inspection.

## 10. Standard Contractual Clauses

10.1. The Standard Contractual Clauses in Appendix 3 shall apply to Customer Personal Data that is transferred from the EU/EEA to a location outside the EU/EEA, either directly or via onward transfer, to any country or recipient: (i) not recognized by the European Commission as providing an adequate level of protection for personal data (as described pursuant to applicable Data Protection Law), and (ii) not covered by a suitable framework recognized by the relevant authorities or courts as providing an adequate level of protection for Personal Data, including but not limited to Binding Corporate Rules for Processors.

10.2. For the purpose of the Standard Contractual Clauses, the Customer shall be deemed to be the “data exporter” and TrafficGuard the “data importer”.

# 11. General Terms

11.1. Without prejudice to the provisions of the Standard Contractual Clauses:

11.1.1. the parties to this Addendum hereby submit to the choice of jurisdiction stipulated in the Service Agreement with respect to any disputes or claims howsoever arising under this Addendum, including disputes regarding its existence, validity or termination or the consequences of its nullity; and

11.1.2. this Addendum and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Service Agreement.

11.2. Nothing in this Addendum reduces TrafficGuard's obligations under the Service Agreement in relation to the protection of Customer Personal Data or permits TrafficGuard to Process (or permit the Processing of) Customer Personal Data in a manner which is prohibited by the Service Agreement. In the event of any conflict or inconsistency between this Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

11.3. Subject to section 11.2, with regard to the subject matter of this Addendum, in the event of inconsistency between the provisions of this Addendum and any other agreements between the parties, including the Service Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this Addendum, the provisions of this Addendum shall prevail.

11.4. Customer may by at least 30 (thirty) calendar days' written notice to TrafficGuard

11.4.1. make any variations to the Standard Contractual Clauses which are required, as a result of any change in, or decision of a competent authority under Data Protection Laws, to allow transfers of Personal Data to be made (or continue to be made) without breach of Data Protection Laws; and

11.4.2. propose any variations to this Addendum which Customer reasonably considers to be necessary to address the requirements of any Data Protection Law.

If Customer gives notice under this section 11.4, the parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing upon and implementing those or alternative variations designed to address the requirements identified in Customer's notice as soon as is reasonably practicable.

11.5. Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties’ intentions as closely as possible or, if

this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

IN WITNESS WHEREOF, this Addendum is entered into and becomes a binding part of the Service Agreement with effect from the date first set out below.

| TrafficGuard (Data Importer) | Customer (Data Exporter) |
| --- | --- |
| Name: | Name: |
| Position: | Position: |
| Authorised Signature: | Authorised Signature: |
| Date: | Date: |

# Appendix 1

This Appendix forms part of the Data Processing Addendum or Standard Contractual Clauses and must be completed and signed by the parties.

**TrafficGuard's Services:** May include, without limitation, digital ad measurement, verification, fraud detection and prevention services intended to intercept invalid traffic at multiple stages of the digital advertising journey including, impression, click and conversion event.

**Scope, type and purpose of the Processing:**

- TrafficGuard process personal (and non-personal) information about End-User engagement with a platform or service the Customer has integrated with our Service. This involves, among other things: (a) the tracking of behaviour of End-Users across a number of the Customer's campaign variables to identify potentially fraudulent traffic (Legitimate interest and compliance with a legal obligation); (b) the tracking of an End-User's journey from the first click or ad impression viewed, through to the achievement of the Customer's goal such as a purchase or install (conversion), in order to ensure determine accurate attribution measurement and identify potentially fraudulent traffic (Legitimate interest and compliance with a legal obligation); (c) produce anonymised data and aggregated data (Legitimate interest); and (d) improve and maintain our services, the Websites and the Service (Consent). By way of example, such data may be used to support the diagnosis of server problems, to identify and create new service offerings and features and to improve our service offerings.

**Duration of the Processing** : For the length of the Agreement until terminated or once processing by TrafficGuard of any End-User data is no longer required for the performance of its relevant obligations under the Agreement.

**Categories of data subjects:** End-User's of the Customer

**Type of Processed Personal Data:**

(a) Non-sensitive:

- **"Technical Information"** : this refers to technical information related to an End-User's mobile device or computer, such as: browser type, device type and model, CPU, system language, memory, OS version, Wi-Fi status, time stamp and zone, device motion parameters and carrier.
- **"Technical Identifiers"** : this refers to various unique identifiers that generally only identify a computer, device, browser or Application. For example, IP address (which may also provide general location information), User agent, IDFA (identifier for advertisers), Android ID (in Android devices); Google Advertiser ID, Customer issued user ID, browser "cookies" other similar unique identifiers.
- **"Engagement Information"** : this refers to information relating to the Customer's ad campaigns and End-User actions, such as: clicks on Customer ads, ad impressions viewed, audiences or segments to which an ad campaign is attributed, the type of ads and the webpage or Application from which such ads were displayed, the webpages on Customer's website visited by an End-User, the URL from the referring website, downloads and installations of Applications, and other interactions, events and actions

Customers choose to measure and analyse within their Application or website (e.g. add to cart, in-app purchases made, clicks, engagement time etc.).

(b) Sensitive: n/a

**Subcontractor that process End-User data:**

The list below identifies Subcontractors, vendors, who process End-User's data on TrafficGuard's behalf. TrafficGuard may update the vendors listed from time to time as appropriate, and may, for the sake of transparency, include vendors that have not yet been deployed. You can find the most current version on our website https://dash.trafficguard.ai .

| Vendor | Purpose |
|---|---|
| AWS | TrafficGuard is hosted on AWS cloud services |
| Google, Inc | TrafficGuard is hosted on GCP cloud services |
| Atlassian | An internal tool used to process data related requests |
| Rollbar | Software TrafficGuard uses to efficiently aggregate error logs |

| TrafficGuard (Data Importer) | Customer (Data Exporter) |
|---|---|
| Name: | Name: |
| Position: | Position: |
| Authorised Signature: | Authorised Signature: |
| Date: | Date: |

# Appendix 2

This Appendix forms part of the Data Processing Addendum or Standard Contractual Clauses and must be completed and signed by the parties.

In the following, the general description of the security measures in respect of TrafficGuard processing the Customer's data is provided.

## 1. Physical access control

Measures to prevent unauthorized persons from gaining access to the data processing systems available in premises and facilities (including databases, application servers and related hardware), where data are processed, including:

General access to the office is controlled by the use of a card access system and cameras are installed throughout the sites. Access is restricted and every individual must be authorized to enter. TrafficGuard employees are trained in all concepts of physical and environmental security.

## 2. Access restriction mechanisms

Measures to prevent data processing systems from being used by unauthorized persons, including:

Admin access is limited to a restricted number of individuals who have individual user ID and password. TrafficGuard maintains password policy that dictates password usage parameters, which mean password needs to have strength, complexity, expiry, reuse, expiration and account lockout. Access to additional individuals is given after the explicit approval of the security team only in extreme circumstances, for a specific purpose, and is limited in duration.

## 3. Data access control

Measures to ensure that persons entitled to use a data processing system gain access to only such Personal Data in accordance with their access rights, and that Personal Data cannot be read, copied, modified or deleted without authorization, including:

Data access is limited to a restricted number of individuals. Every employee has a unique user ID and password and all access rights for user accounts are managed by IT/Ops/Security personnel and controlled with tools to protect unauthorized access. Personal data cannot be changed or deleted by an unauthorized person.

## 4. Communication and transport control

Measures to ensure that data cannot be read, copied, modified or deleted without authorization during electronic transmission, including:

TrafficGuard maintains firewalls and encryption technologies to protect gateways and pipelines through which data travels. All personal data that are in transport are logged, encrypted and transmitted across SSL protected channels. Only IT, Security and Engineering personnel can audit that transaction.

## 5. Entry control

Measures to monitor whether data have been entered, changed or removed (deleted), and by whom, from data processing systems via logging and reporting capabilities, including:

TrafficGuard uses Amazon AWS data centre policy, physical access to data processing areas is not permitted. Action performed within the software application are logged and can not be changed or deleted.

## 6. Processing control

The following measures to ensure that data are processed solely in accordance with the instructions of the Customer, including:

All employees that are responsible for the processing of personal data are trained to ensure that personal data is processed in accordance with Data exporter instructions.

## 7. Availability contro l

Measures to ensure that Personal Data is protected against accidental destruction or loss (physical/logical), including:

TrafficGuard performs regular testing to ensure that availability supporting system function properly. All procedures are documented and approved by management, which includes incident response, data backup, disaster recovery too and are designed to maintain business operation.

## 8. Separation control

Measures to ensure that the collected data can be processed separately for different purposes, including:

Personal data is restricted by user access and authorization control, application data and access to database content are defined by a unique account. TrafficGuard maintains separate environments for development and testing, for research and development; and for production system and data.

| TrafficGuard (Data Importer) | Customer (Data Exporter) |
|---|---|
| Name: | Name: |
| Position: | Position: |
| Authorised Signature: | Authorised Signature: |
| Date: | Date: |

EUROPEAN COMMISSION
DIRECTORATE-GENERAL JUSTICE

Directorate C: Fundamental rights and Union citizenship
**Unit C.3: Data protection**

**Commission Decision C(2010)593**
**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

Name of the data exporting organisation:

Address:

Tel.: ; e-mail:

Other information needed to identify the organisation:

……
(the data **exporter**)

And

Name of the data importing organisation: **TrafficGuard Pty Ltd**

Address: Suite 10, 16 Brodie Hall Drive, Technology Park, WA 6102 Bentley, Australia

Tel.: +61 8 9473 2500; e-mail: privacy@trafficguard.ai

Other information needed to identify the organisation: ABN 66 126 813 214

……
(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[1];

(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.

[1] Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

*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 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 wit hin 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 servic es 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[2]***

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:

---

[2] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia,* internationally recognised sanctions, tax - reporting requirements o r anti - money - laundering reporting requirements.

(i) any legally bi nding 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 b y 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 successo r 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, namely

*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 s ubcontract 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 d ata 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[3]. 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, namely

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

[3] This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

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…….

(stamp of organisation)

**On behalf of TrafficGuard (Data Importer) :**

Name:

Position:

Address: Suite 10, 16 Brodie Hall Drive, Technology Park, WA 6102 Bentley, Australia

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

Signature

(stamp of organisation)