Infomedia GDPR Model Clause Data Processing Agreement

By and Between

Name of Dealer:
("**Data Controller**") with offices at
AND

Infomedia Ltd, A.C.N. 003 326 243 an Australian corporation with offices at 3 Minna Close, Belrose, NSW 2085 Australia ("**Data Processor**")

WHEREAS

a) Dealer has entered into an End User Licence Agreement with Infomedia and wishes to transfer personal data of a Data Subject located in the European Union to Infomedia for processing by Infomedia in Australia (and elsewhere by sub-processors of Infomedia) under the Model Clauses approved by the European Commission.

b) Infomedia agrees to process that personal data under the terms of this Data Processing Agreement

1. DEFINITIONS

Unless defined in the End User Licence Agreement, all capitalized terms used in this Agreement shall have the meanings given to them below:

1.1 **Agreement:** means this Data Processing Agreement.

1.2 **Applicable Data Protection Law**: means the following data protection law(s)): (i) where Data Controller is established in a European Economic Area ("EEA") member state or where Data Controller's Agents or End-Users access the Services from an EEA member state: (a) prior to May 25, 2018, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, entitled "On the protection of individuals with regard to the processing of personal data, and on the free movement of such data." (as implemented into the relevant national laws of the member state in which Data Controller is established), and (b) on and after May 25, 2018, EU Regulation 2016/679 (and any applicable national laws made under it); and (ii) where Data Controller is established in Switzerland, the Swiss Federal Act of 19 June 1992 on Data Protection (as may be amended or superseded).

1.3 **Data Processor:** has the meaning given in Applicable Data Protection Law (and, for the purposes of this Agreement, means Infomedia).

1.4 **Data Subject:** means an individual who is the subject of Personal Data.

1.5 **End User Licence Agreement**: means the software licence agreement between Data Controller and Data Processor for the provision of the Service(s).

1.6 **Party:** means any of Data Controller or Data Processor, and "Parties" means Data Controller and Data Processor.

1.7 **Personal Data**: means any information relating to an identified or identifiable natural person, where an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

1.8 **Privacy Shield Framework:** means the EU-U.S. and/or Swiss-U.S. Privacy Shield self-certification program operated by the US Department of Commerce.

1.9 **Privacy Shield Principles:** means the Privacy Shield Framework Principles (as supplemented by the Supplemental Principles) contained in Annex II to the European Commission Decision C(2016)4176 of July 12, 2016 (as may be amended, superseded, or replaced).

1.10 **Processing:** means any operation or set of operations which is performed upon Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or

alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.11 **Processor Group:** means Data Processor and any entity which controls, is controlled by, or is under common control with, Data Processor.

1.12 **Service(s):** means the products and services that are ordered by Data Controller through a link or via an Order Form and made available online by Data Processor, via the applicable subscriber login link and other web pages designated by Data Processor.

1.13 **Service Data:** means electronic data, text, messages, communications or other materials submitted to and stored within the Service by Data Controller, its Agents and End- Users in connection with Data Controller's use of such Service, including, without limitation, Personal Data.

1.14 **Sub-processor**: means any third-party data processor engaged by Data Processor, including entities from the Processor Group, who receives Personal Data from Data Processor for processing on behalf of Data Controller and in accordance with Data Controller's instructions (as communicated by Data Processor) and the terms of its written subcontract.

1.15 **Supervisor:** means the Data Protection Supervisory Authority with competence over Data Controller's and Data Processor's Processing of Personal Data.

In addition to the above, any other capitalized terms used but not defined in this Agreement shall have the meaning set forth in the End User Licence Agreement.

2. PURPOSE

2.1 Data Controller and Data Processor have entered into End User Licence Agreements pursuant to which Data Controller is granted a license to access and use the Service. In providing the Service, Data Processor will engage, on behalf of Data Controller, in the Processing of Personal Data submitted to and stored within the Service by Data Controller or third parties with whom Data Controller transacts using the Service.

2.2 The Parties are entering into this Agreement to ensure that the Processing by Data Processor of Personal Data, within the Service by Data Controller and/or on its behalf, is done in a manner compliant with Applicable Data Protection Law and its requirements regarding the collection, use and retention of Personal Data of Data Subjects.

3. OWNERSHIP OF THE SERVICE DATA

As between the Parties, all Service Data Processed under the terms of this Agreement and the End User Licence Agreement shall remain the property of Data Controller. Under no circumstances will Data Processor act, or be deemed to act, as a "controller" (or equivalent concept) of the Service Data Processed within the Service under any Applicable Data Protection Law.

4. OBLIGATIONS OF DATA PROCESSOR

4.1 The Parties agree that the subject-matter and duration of Processing performed by Data Processor under this Agreement, including the nature and purpose of Processing, the type of Personal Data, and categories of Data Subjects, shall be as described in the End User Licence Agreement.

4.2 As part of Data Processor providing the Service to Data Controller under the End User Licence Agreement, Data Processor agrees and declares as follows:

(i) to process Personal Data in accordance with Data Controller's documented instructions as set out in this Agreement or as otherwise necessary to provide the Service, except where required otherwise by applicable laws (and provided such laws do not conflict with Applicable Data Protection Law); in such case, Data Processor shall inform Data Controller of that legal requirement upon becoming aware of the same (except where prohibited by applicable laws);

(ii) to ensure that all staff and management of any member of the Processor Group are fully aware of their responsibilities to protect Personal Data in accordance with this Agreement and have

committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(iii)   to implement and maintain appropriate technical and organizational measures to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access (a "Data Security Breach"), provided that such measures shall take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, so as to ensure a level of security appropriate to the risks represented by the Processing and the nature of the Data to be protected;

(iv)   to notify Data Controller, without undue delay, in the event of a confirmed Data Security Breach affecting Data Controller's Service Data and to cooperate with Data Controller as necessary to mitigate or remediate the Data Security Breach;

(v)   to comply with the requirements of Section 5 (Use of Sub-processors) when engaging a Sub-processor;

(vi)   taking into account the nature of the Processing, to assist Data Controller (including by appropriate technical and organizational measures), insofar as it is commercially reasonable, to fulfil Data Controller's obligation to respond to requests from Data Subjects to exercise their rights under Applicable Data Protection Law (a "Data Subject Request"). In the event Data Processor receives a Data Subject Request directly from a Data Subject, it shall (unless prohibited by law) direct the Data Subject to the Data Controller in the first instance. However, in the event Data Controller is unable to address the Data Subject Request, taking into account the nature of the Processing and the information available to Data Processor, Data Processor, shall, on Data Controller's request and at Data Controller's reasonable expense, address the Data Subject Request, as required under the Applicable Data Protection Law;

(vii)   upon request, to provide Data Controller with commercially reasonable information and assistance, taking into account the nature of the Processing and the information available to Data Processor, to help Data Controller to conduct any data protection impact assessment or Supervisor consultation it is required to conduct under Applicable Data Protection Law;

(viii)   upon termination of Data Controller's access to and use of the Service, to comply with the requirements of Section 9 (Return and Destruction of Personal Data);

(ix)   to comply with the requirements of Section 6 (Audit) in order to make available to Data Controller information that demonstrates Data Processor's compliance with this Agreement; and

(x)   to appoint a security officer who will act as a point of contact for Data Controller, and coordinate and control compliance with this Agreement, including the measures detailed in Exhibit A to this Agreement.

4.3 Data Processor shall immediately inform Data Controller if, in its opinion, Data Controller's Processing instructions infringe any law or regulation. In such event, Data Processor is entitled to refuse Processing of Personal Data that it believes to be in violation of any law or regulation.

5.   USE OF SUB-PROCESSORS

5.1 Data Controller agrees that Data Processor may appoint Sub-processors to assist it in providing the Service and Processing Personal Data provided that such Sub-processors:

(i)   agree to act only on Data Processor's instructions when Processing the Personal Data (which instructions shall be consistent with Data Controller's Processing instructions to Data Processor); and

(ii)   agree to protect the Personal Data to a standard consistent with the requirements of this Agreement, including by implementing and maintaining appropriate technical and organizational measures to

protect the Personal Data they Process consistent with the Security Standards described in Exhibit A.

5.2   Data Processor agrees and warrants to remain liable to Data Controller for the subcontracted Processing services of any of its direct or indirect Sub-Processors under this Agreement. Data Processor shall maintain an up-to-date list of the names and location of all Sub-Processors used for the Processing of Personal Data under this Agreement at http://www.infomedia.com.au/gdpr/ and also available upon request to privacy@Infomedia.com. Data Processor shall update the list on its website of any Sub-Processor to be appointed prior to the date on which the Sub-Processor shall commence processing Personal Data. Customer may sign up to receive email notifications of any such changes.

5.3   In the event that Data Controller objects (on reasonable grounds) to the Processing of its Personal Data by any newly appointed Sub-Processor as described in Section 5.2, it shall inform Data Processor within five days of Data Processor providing notice of the appointment or intended appointment. In such event, Data Processor will work with Data controller in good faith to make available a commercially reasonable change in the provision of the Services which avoids the use of that proposed Sub-processor. Where such change cannot be made within 30 days from Data Processor's receipt of notice from the Data Controller, then despite anything else in this agreement or any other agreement pertaining to the Services, either party may terminate the Services by giving written notice to the other party. Termination will take effect immediately and Data Processor will provide Data Controller with a pro rata reimbursement of any sums paid in advance for Services to be provided but not yet received by Data Controller as of the effective date of termination.

5.4   In addition, and as stated in the End User Licence Agreement, the Service provides links to integrations with Third Party Services, including, without limitation, certain Third Party Services which may be integrated directly into Data Controller's account or instance in the Service. If Data Controller elects to enable, access or use such Third Party Services, its access and use of such Third Party Services is governed solely by the terms and conditions and privacy policies of such Third Party Services, and Data Processor does not endorse, is not responsible or liable for, and makes no representations as to any aspect of such Third Party Services, including, without limitation, their content or the manner in which they handle Service Data (including Personal Data) or any interaction between Data Controller and the provider of such Third Party Services. Data Processor is not liable for any damage or loss caused or alleged to be caused by or in connection with Data Controller's enablement, access or use of any such Third Party Services, or Data Controller's reliance on the privacy practices, data security processes or other policies of such Third Party Services. The providers of Third Party Services shall not be deemed Sub-processors for any purpose under this Agreement.

6.   AUDIT

6.1 The Parties acknowledge that Data Processor uses external auditors to verify the adequacy of its security measures and the audit will comply with the details set out in Clause 3 Appendix 3.

7. INTERNATIONAL DATA EXPORTS

7.1   Data Controller acknowledges that Data Processor and its Sub-processors may maintain data processing operations in countries that are outside of the EEA and Switzerland. As such, both Data Processor and its Sub-processors may Process Personal Data in non-EEA and non-Swiss countries. This will apply even where Data Controller has agreed with Data Processor to host Personal Data in the EEA if such non-EEA Processing is necessary to provide support-related or other services requested by Data Controller.

7.2   Where Data Controller is self-certified to the Privacy Shield Framework and transfers Personal Data from the EEA or Switzerland to Data Processor, Data Controller is obliged under the terms of the Privacy Shield Framework to flow down the following requirements and Data Processor hereby agrees:

   (i)   to provide at least the same level of protection to such Personal Data as is required by the Privacy Shield Principles;

   (ii)   to notify Data Controller if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Privacy Shield Principles; and

(iii)   upon notice, including under Section 7.2(ii) above, to work with Data Controller to take reasonable and appropriate steps to stop and remediate any unauthorized processing of the Personal Data.

7.3   Where Data Controller is not self-certified to the Privacy Shield Framework, this section shall apply in place of Section 7.2 above. Where Data Processor Processes or permits any Sub-processor to Process Personal Data outside the EEA or Switzerland, Data Processor shall comply with the EU Commission's "Controller-to-Processor Model Clauses" (annexed to EU Commission Decision 2010/87/EU). The Parties have agreed to practical interpretations of certain provisions contained within the Controller-to-Processor Model Clauses, as permitted by the Article 29 Working Party. These interpretations clarify how Data Processor should implement the Model Clauses in practice, and are set out in Appendix 3 to this Agreement.

7.4   The Parties agree that each Party may disclose any relevant privacy provisions in this Agreement to the US Department of Commerce, the Federal Trade Commission or a relevant European Data Protection Supervisory Authority.

8.   OBLIGATIONS OF DATA CONTROLLER

As part of Data Controller receiving the Service, Data Controller agrees and declares as follows:

(i)   it is solely responsible for the accuracy of Personal Data and the means by which such Personal Data is acquired and the Processing of Personal Data by Data Controller, including instructing Processing by Data Processor in accordance with this Agreement, is and shall continue to be in accordance with all the relevant provisions of the Applicable Data Protection Law, particularly with respect to the security, protection and disclosure of Personal Data;

(ii)   that if Processing by Data Processor involves any "special" or "sensitive" categories" of Personal Data (as defined under Applicable Data Protection Law), Data Controller has collected such Personal Data in accordance with Applicable Data Protection Law;

(iii)   that Data Controller will:

(a)   inform its Data Subjects about its use of data processors to Process their Personal Data, including Data Processor and that their Personal Data may be Processed outside of the European Economic Area; and

(b)   will obtain the express and legally binding consent of the Data Subjects allowing the Data Controller to process the Data Subjects' data on the basis described in this DPA;

(iv)   that it shall respond in reasonable time and to the extent reasonably practicable to enquiries by Data Subjects regarding the Processing of their Personal Data by Data Controller, and to give appropriate instructions to Data Processor in a timely manner; and

(v)   that it shall respond in a reasonable time to enquiries from a Supervisor regarding the Processing of relevant Personal Data by Data Controller.

9.   RETURN AND DESTRUCTION OF PERSONAL DATA

Upon the termination of Data Controller's access to and use of the Service, Data Processor will up to thirty (30) days following such termination permit Data Controller to export its Service Data, at its expense, in accordance with the capabilities of the Service. Following such period, Data Processor shall have the right to delete all Service Data stored or Processed by Data Processor on behalf of Data Controller in accordance with Data Processor's deletion policies and procedures. Data Controller expressly consents to such deletion. Each Data Processor may retain the Service Data to the extent required by law (but only to the extent and duration necessary to comply with such laws) provided the Data Processor ensures that the Service Data is processed as necessary for the purpose(s) specified in the applicable laws requiring its storage and for no other purpose.

10.   DURATION

This Agreement will remain in force as long as Data Processor Processes Personal Data on behalf of Data Controller in connection with the Service.

11. NO CONSEQUENTIAL DAMAGES; LIMITATION ON LIABILITY

11.1 UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY (WHETHER IN CONTRACT, TORT, NEGLIGENCE OR OTHERWISE) WILL EITHER PARTY TO THIS AGREEMENT, OR THEIR AFFILIATES. OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SERVICE PROVIDERS, SUPPLIERS OR LICENSORS BE LIABLE TO THE OTHER PARTY OR ANY THIRD PARTY FOR ANY LOST PROFITS, LOST SALES OR BUSINESS, LOST DATA (BEING DATA LOST IN THE COURSE OF TRANSMISSION VIA DATA CONTROLLER'S SYSTEMS OR OVER THE INTERNET THROUGH NO FAULT OF DATA PROCESSOR), BUSINESS INTERRUPTION, LOSS OF GOODWILL, OR FOR ANY TYPE OF INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, CONSEQUENTIAL OR PUNITIVE LOSS OR DAMAGES, OR ANY OTHER LOSS OR DAMAGES INCURRED BY THE OTHER PARTY OR ANY THIRD PARTY IN CONNECTION WITH THIS AGREEMENT, OR THE SERVICES, REGARDLESS OF WHETHER SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF OR COULD HAVE FORESEEN SUCH DAMAGES.

11.2 NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THIS AGREEMENT OR THE END USER LICENCE AGREEMENT, DATA PROCESSOR'S AGGREGATE LIABILITY TO DATA CONTROLLER OR ANY THIRD PARTY ARISING OUT OF THIS AGREEMENT AND ANY LICENSE, USE OR EMPLOYMENT OF THE SERVICE, SHALL IN NO EVENT EXCEED THE LIMITATIONS SET FORTH IN THE END USER LICENCE AGREEMENT.

11.3 FOR THE AVOIDANCE OF DOUBT, THIS SECTION SHALL NOT BE CONSTRUED AS LIMITING THE LIABILITY OF EITHER PARTY WITH RESPECT TO CLAIMS BROUGHT BY DATA-SUBJECTS.

12. MISCELLANEOUS

This Agreement may not be amended or modified except by a writing signed by both Parties hereto. This Agreement may be executed in counterparts. The terms and conditions of this Agreement are confidential and each party agrees and represents, on behalf of itself, its employees and agents to whom it is permitted to disclose such information that it will not disclose such information to any third party; provided, however, that each party shall have the right to disclose such information to its officers, directors, employees, auditors, attorneys and third party contractors who are under an obligation to maintain the confidentiality thereof and further may disclose such information as necessary to comply with an order or subpoena of any administrative agency or court of competent jurisdiction or as reasonably necessary to comply with any applicable law or regulation. Data Controller may not, directly or indirectly, by operation of law or otherwise, assign all or any part of its rights under this Agreement or delegate performance of its duties under this Agreement without Data Processor's prior consent, which consent will not be unreasonably withheld. Data Processor may, without Data Controller's consent, assign this Agreement to any affiliate or in connection with any merger or change of control of Data Processor or the sale of all or substantially all of its assets provided that any such successor agrees to fulfil its obligations pursuant to this Agreement. Subject to the foregoing restrictions, this Agreement will be fully binding upon, inure to the benefit of and be enforceable by the Parties and their respective successors and assigns. This Agreement and the End User Licence Agreement constitute the entire understanding between the Parties with respect to the subject matter herein, and shall supersede any other arrangements, negotiations or discussions between the Parties relating to that subject-matter.

13. GOVERNING LAW AND JURISDICTION

This Agreement is governed by the laws of England and is subject to the exclusive jurisdiction of the courts of England.

14. NOTICES

Notices under this Agreement should be sent to:

a) The Data Controller at the address set out on the first page; and

b) Infomedia Ltd, Attn: Legal Department, 3 Minna Close, Belrose, NSW 2085 Australia or by email legal@infomedia.com.au

IN WITNESS WHEREOF, the Parties hereto have executed this Agreement by their duly authorized officers or representatives as of the last date of execution below ("Effective Date"):

For and on behalf of DATA CONTROLLER:	For and on behalf of INFOMEDIA Ltd (DATA PROCESSOR)
By:	By:
Name:	Name: Mark Grodzicky
Title:	Title: Company Secretary
Date:	Date:

Exhibit A Security Standards

As of the Effective Date of this Agreement, Data Processor, when Processing Personal Data on behalf of Data Controller in connection with the Service, Data Processor shall implement and maintain the following technical and organizational security measures for the Processing of such Personal Data ('Security Standards"):

1. **Physical Access Controls**: Data Processor shall take reasonable measures to prevent physical access, such as secured buildings and access controls within premises, to prevent unauthorized persons from gaining access to Personal Data, and ensure Third Parties such as those operating data centers also are adhering to such controls.

2. **System Access Controls:** Data Processor shall take reasonable measures to prevent Personal Data from being used without authorization. These controls shall vary based on the nature of the Processing undertaken and may include, among other controls, authentication via passwords and/or two-factor authentication, documented authorization processes, documented change management processes and/or, logging of access on several levels.

3. **Data Access Controls:** Data Processor shall take are reasonable measures to provide that Personal Data is accessible and manageable only by properly authorized staff, direct database query access is restricted and application access rights are established and enforced to ensure that persons entitled to use a data processing system only have access to the Personal Data to which they have privilege of access; and, that Personal Data cannot be read, copied, modified or removed without authorization in the course of Processing.

4. **Transmission Controls:** Data Processor shall take reasonable measures to ensure that it is possible to check and establish to which entities the transfer of Personal Data by means of data transmission facilities is envisaged so Service Data cannot be read, copied, modified or removed without authorization during electronic transmission or transport.

5. **Input Controls:** Data Processor shall take reasonable measures to provide that it is possible to check and establish whether and by whom Service Data has been entered into data processing systems, modified or removed. Data Processor shall take reasonable measures to ensure that (i) the Personal Data source is under the control of Data Controller; and (ii) Personal Data integrated into the Service is managed by secured transmission from Data Controller.

6. **Data Backup:** Back-ups of the databases in the Service taken on a regular basis, are secured, and encrypted to ensure that Personal Data is protected against accidental destruction or loss when hosted by Data Processor.

7. **Logical Separation:** Data from different Data Processor's subscriber environments is logically segregated on Data Processor's systems to ensure that Personal Data that is collected for different purposes may be Processed separately.

Exhibit B

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 organization:

Address

Email:

Other information needed to identify the organization

(the data exporter)

And

Name of the data importing organization: Infomedia Ltd including IFM Europe Limited and IFM America's Inc

Address: 3 Minna Close, Belrose, NSW 2085 Australia

Email: privacy@Infomedia.com.au

(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.

1.   **Definitions**

For the purposes of the Clauses:

'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;

'the data exporter' means the controller who transfers the personal data;

'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;

'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;

'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;

'technical and organizational 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.

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.

3. Third-party beneficiary clause

3.1   The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5 (a) to (e), and (g) to G), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

3.2   The data subject can enforce against the data importer this Clause, Clause S(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.

3.3   The data subject can enforce against the subprocessor this Clause, Clause S(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.

3.4   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.

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, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

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

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

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

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

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

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

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 unauthorised access, and

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

(e)   to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

6. Liability

6.1 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.

6.2 If a data subject is not able to bring a claim for compensation in accordance with paragraph I 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 or by operation of law, in which case the data subject can enforce its rights against such entity.

6.3 The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

6.4 If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs I 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.

7. Mediation and jurisdiction

7.1 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.

7.2   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.

8.   Cooperation with supervisory authorities

8.1   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.

8.2   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.

8.3   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).

9.   Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

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 Clauses.

11.   Subprocessing

11.1   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.

11.2   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 I 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.

11.3   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.

11.4   The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 G), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

12. Obligation after the termination of personal data processing services

12.1. 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.

12.2 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.

For and on behalf of DATA EXPORTER:	For and on behalf of INFOMEDIA Ltd (DATA IMPORTER)
By:	By:
Name:	Name: Mark Grodzicky
Title:	Title: Company Secretary
Date:	Date:

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 importer

The data importer is (*please specify briefly your activities relevant to the transfer):* The data importer operates a cloud-based automotive parts and service services platform, including an online helpdesk ticketing service, cloud-based customer support live chat platform, self-service options and customer-support features. Further information can be found online at www.infomedia.com.au

Data exporter

The data exporter is (*please specify briefly activities relevant to the transfer):* The data exporter is a customer, subscriber to and / or user of Infomedia and uses the Infomedia cloud based automotive parts and service services platform to service for its end user customers (eg owner of the cars).

Data subjects

The personal data transferred concern the following categories of data subjects (*please specify*): service technicians, end user customers, internal staff

Categories of data

The personal data transferred concern the following categories of data (*please specify*): names, email addresses, phone numbers, IP addresses, car vin and registration numbers

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (*please specify*): none

Processing operations

The personal data transferred will be subject to the following basic processing activities (*please specify*): The data importer will host and process personal data in the course of providing its cloud-based customer services, helpdesk platform services, and its cloud-based customer support live chat platform services to data exporter.

For and on behalf of DATA EXPORTER:	For and on behalf of INFOMEDIA Ltd (DATA IMPORTER)
By:	By:
Name:	Name: Mark Grodzicky
Title:	Title: Company Secretary
Date:	Date:

Appendix 2 to the Standard Contractual Clauses

Data importer (and any subprocessor to data importer) shall implement the technical and organizational measures described in Exhibit A to the Data Processing Agreement executed between data exporter and data importer.

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

For and on behalf of DATA EXPORTER:	For and on behalf of INFOMEDIA Ltd (DATA IMPORTER)
By:	By:
Name:	Name: Mark Grodzicky
Title:	Title: Company Secretary
Date:	Date:

Appendix 3 to the Standard Contractual Clauses

Where the EU Controller-to-Processor Model Clauses ("Clauses") apply pursuant to Section 7 of this Data Processing Agreement, then this Appendix 3 sets out the parties' interpretations of their respective obligations under specific provisions within the Clauses, as identified below. Where a party complies with the interpretations set out in this Appendix 3, that party shall be deemed by the other party to have complied with its commitments under the Clauses. When used below, the terms "data exporter" and "data importer" shall have the meaning given to them in the Clauses.

Nothing in the interpretations below is intended to vary or modify the Clauses or conflict with either party's rights or responsibilities under the Clauses and, in the event of any conflict between the interpretations below and the Clauses, the Clauses shall prevail to the extent of such conflict. Notwithstanding this, the parties expressly agree that any claims brought under the Clauses shall be exclusively governed by the limitations on liability set out in Section 11 of this Data Processing Agreement. For the avoidance of any doubt, in no event shall any party limit its liability with respect to any data subject rights under the Clauses.

1. **Interpretation of Data Exporter Obligations pursuant to Clause 4 with respect to Nondisclosure Requirements.**

1.1 Data exporter agrees that these Clauses constitute data importer's Confidential Information under the confidentiality provisions of the data importer's End User Licence Agreement and may not be disclosed by data exporter to any third party without data importer's prior agreement (other than to a data subject pursuant to Clause 4(h) or a supervisory authority pursuant to Clause 8).

2. **Interpretation of Data Exporter's Right to Suspend Data Transfer or Terminate the Contract After Notice and Opportunity to Cure in accordance with Clause 5 (a):**

2.1 The parties acknowledge that data importer may process the Personal Data only on behalf of the data exporter and in compliance with its instructions as provided by the data exporter and the Clauses.

2.2 The parties acknowledge that if data importer 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.

2.3 Accordingly, the data exporter shall provide notice to data importer of its intent to suspend the transfer of Personal Data and/or terminate the contract and provide data importer with sufficient opportunity to cure the non-compliance ("Cure Period"). If after the Cure Period, the data importer cannot cure the non-compliance then the data exporter may exercise its right to suspend the transfer of Personal Data and/or terminate the contract.

2.4 Paragraph 3 above shall not apply in circumstances where there is an urgent need to suspend the transfer of Personal Data and/or terminate the contract due to a serious risk of harm to data subjects. In this event, the parties acknowledge that the data exporter shall be entitled to suspend the transfer of Personal Data and/or terminate the contract immediately.

3. **Interpretation of the Audit of Technical and Organizational Measures implemented by the Data importer in accordance with Clause 5 (f):**

3.1 The parties acknowledge that the data importer and its sub-processors that use external auditors to verify the adequacy of security measures, including the security of the physical data centres from which subprocessors provide its data processing services. This audit:

    (a)   will be performed at least annually;

    (b)   will be performed according to ISO 27001 standards or such other alternative standards that are substantially equivalent to ISO 27001;

      (c)   will be performed by independent third party security professionals at data importer's selection and expense; and

      (d)   will result in the generation of an audit report affirming that data importer's subprocessor's data security controls achieve prevailing industry standards (including, without limitation, Service Organization Controls No. 2 (SOC2) in accordance with auditing standards in the Statements on Standards for Attestation Engagements No. I 6 (SSAE 16)) or such other alternative standards that are substantially equivalent to ISO 27001 ("Report");

3.2   Data importer shall provide responsive and detailed information to data exporter's requests for information (including any requests by data exporter under instruction from data subjects), which may include responses to relevant information security and audit questionnaires;

3.3   At data exporter's written request, data importer will provide data exporter with a confidential summary of the Report ("Summary Report") so that data exporter can reasonably verify data importer's compliance with the security and audit obligations under the Clauses. The Summary Report will constitute data importer's Confidential Information.

3.4   Data exporter agrees to exercise its audit right under Clause 5 (f) by instructing data importer to execute the audit measures as described in this Appendix.

4.   **Interpretation of the Obligation of Data Importer to Provide Any Onward Subprocessor Agreement in accordance with Clause 5(j):**

4.1   The parties acknowledge the obligation of the data importer to send promptly a copy of any onward subprocessor agreement it concludes under the Clauses to the data exporter.

4.2   Accordingly, the parties agree that upon the request of data exporter, data importer shall provide all relevant information evidencing compliance with Clause 5 (j). Should the information provided by data importer be insufficient to demonstrate data importer's compliance with Clause 5 (j then data importer may provide a version of the onward subprocessor agreement with commercially sensitive and/or confidential information removed.

4.3   Accordingly, the parties agree that any onward subprocessor agreement or information related thereto that data importer provides to data exporter shall constitute data importer's Confidential Information under data importer's End User Licence Agreement and shall not be disclosed by data exporter to any third party without data importer's prior agreement.

5.   **Interpretation of Liability requirements as between the Data Exporter and Data Importer pursuant to Clause 6**

5.1   Any claims brought under the Clauses shall be subject to the terms and conditions, including but to limited to, the. exclusions and limitations set forth in data importer's End User Licence Agreement. In no event shall any party limit its liability with respect to any data subject rights under these Clauses.

6.   **Interpretation of the Onward Sub-processing implemented by the Data importer in accordance with Clause 11:**

6.1   The parties acknowledge that, pursuant to FAQ II.I in Article 29 Working Party Paper WP 176 entitled "FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC" the data exporter may provide a general consent to onward sub-processing by the data importer.

6.2   Accordingly, data exporter provides a general consent to data importer, pursuant to Clause 11 of these Clauses, to engage onward sub-processors. Such consent is conditional on data importer's compliance with the sub-processing conditions set forth in Section 5 of the Data Processing Agreement entered into between data exporter and data importer, as well as the requirements set out below, which collectively

ensure that the onward subprocessor is subject to the same data protection obligations as the data importer:

(a)   any such onward sub-processor must agree in writing:

    (i)   to only process Personal Data in the European Economic Area or another country that the European Commission has formally recognized as having an "adequate" level of protection in accordance with the requirements of EU Directive 95/46/EC; or

    (ii)   to process Personal Data on terms equivalent to these Clauses, pursuant to Privacy Shield requirements or equivalent, or pursuant to a Binding Corporate Rules approval by European data protection authorities and whose scope extends to transfers of Personal Data from the territories in which the data exporter is established;

(b)   data importer restricts the onward sub-processor's access to Personal Data only to what is strictly necessary to perform its subcontracted data processing services to data importer (which shall be consistent with the instructions issued to data importer by data exporter) and data importer will prohibit the onward sub-processor from processing the Personal Data for any other purpose.