

Terms of Use

The following terms and conditions govern all use of the WildlifeTradePortal.org website and all content and services available at or through the website (collectively, the "Portal"). The Portal is owned and operated by TRAFFIC International ("TRAFFIC"). The Portal is offered subject to your acceptance without modification of all of the terms and conditions contained herein and in all other operating rules, policies and procedures that may be published from time to time on the Portal by TRAFFIC (collectively, the "Information Sharing Agreement" or the "Agreement").

Please read this Agreement carefully before accessing or using the Portal. By accessing or using any part of the Portal you agree to become bound by the terms and conditions of this Agreement, which form a legally binding contract between you and TRAFFIC. If you do not agree to all the terms and conditions of this Agreement, then you may not access the Portal or use any services. If you are using the Portal on behalf of an employer or another entity, you represent and warrant that you have the authority and capacity to bind such entity to the Agreement.

THIS AGREEMENT IS MADE BY AND BETWEEN:

- (1) TRAFFIC International, a charity registered in the United Kingdom with registered charity number 1076722, whose registered headquarters are located at The David Attenborough Building, Pembroke Street, Cambridge CB2 3QZ ("**TRAFFIC**"); and
 - (2) The user of the Portal (the "**User**");
- (each a "**Party**" and together the "**Parties**").

BACKGROUND

- A. The purpose of the Agreement is to establish a working relationship between TRAFFIC and the User for the purposes of sharing data relating to the illegal wildlife trade.
- B. The aim of the information exchange on the Portal is to facilitate the collection of data on wildlife trade to enable both TRAFFIC and the User to build up an overall picture of the situation at a local, national and international level. Analysis of the gathered information will aid the Parties' work in combating the illegal and/or unsustainable trade and consumption of wildlife. It will enable the Parties to increase their insight into and understanding of wildlife crime and to drive enforcement action in the hotspots for poaching and illegal trade, specifically targeting the key players and organisations involved.
- C. This Agreement sets out the data protection terms that will apply to any such transfer or information release, in order to ensure that the data protection rights and freedoms of individuals (as understood in the GDPR) remain protected in accordance with Applicable Data Protection Law.

In consideration of the Parties' mutual obligations contained within this Agreement, the Parties agree as follows:

1. Definitions

1.1. In this Clause, the following terms shall have the following meanings:

- (a) "controller", "processor", "data subject", "personal data", "processing" (and "process") and "special categories of personal data" shall have the meanings given in EU Data Protection Law;
- (b) "**Applicable Data Protection Law**" means all worldwide data protection and privacy laws and regulations applicable to the personal data in question, including, where applicable, EU Data Protection Law;
- (c) "**Controller to Controller Model Clauses**" means the model clauses for the transfer of Personal Data to Controllers established in third countries approved by the European Commission from time to time, the approved version of which in force at present is that set out in the European Commission's Decision 2004/915/EC of 27 December 2004;
- (d) "**Data Processing Activities**" means the activities carried out by the User in relation to the processing of personal data as described in Appendix II;
- (e) "**Effective Date**" means the date upon which the User registered an account on the Portal;
- (f) "**EU Data Protection Law**" means (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (General Data Protection Regulation) (the "**GDPR**"); (ii) the EU e-Privacy Directive (Directive 2002/58/EC); and (iii) any and all applicable national data protection laws made under or pursuant to (i) or (ii); in each case as may be amended or superseded from time to time; and
- (g) "**Permitted Purpose**" means the purpose for which the personal data is being transferred, as described in Appendix II.

2. Website Use Restrictions

- 2.1. The User shall not, nor permit anyone else to, directly or indirectly: (i) reverse engineer, disassemble, decompile or otherwise attempt to discover the source code or underlying algorithms of all or any part of the Portal (except that this restriction shall not apply to the limited extent restrictions on reverse engineering are prohibited by applicable local law); (ii) modify or create derivatives of any part of the Portal; (iii) rent, lease, or use the Portal for timesharing or service bureau purposes; or (iv) remove or obscure any proprietary notices on the Portal. As between the Parties, TRAFFIC shall own all title, ownership rights, and intellectual property rights in and to the Portal, and any copies or portions thereof.
- 2.2. The User shall not use any "deep-link", "page-scrape", "robot", "spider" or other automatic device, program, algorithm or methodology, or any similar or equivalent manual process, to access, acquire, copy or monitor any portion of the Portal or any of its content, or in any way reproduce or circumvent the navigational structure or presentation of the Portal or any of its content, to obtain or attempt to obtain any materials, documents or information through any means not purposely made available through the Portal. TRAFFIC reserves the right to bar any such activity.
- 2.3. The User shall not attempt to gain unauthorised access to any portion or feature of the Portal, or any other systems or networks connected to the Portal or to any TRAFFIC server, or to any of the services offered on or through the Portal, by hacking, password "mining", or any other illegitimate means.
- 2.4. The User shall not probe, scan or test the vulnerability of the Portal or any network connected to the Portal, nor breach the security or authentication measures on the Portal or any network connected to the Portal.
- 2.5. The User shall not take any action that imposes an unreasonable or disproportionately large load on the infrastructure of the Portal or TRAFFIC's systems or networks, or any systems or networks connected to the Portal or to TRAFFIC.
- 2.6. The User shall not use any device, software or routine to interfere or attempt to interfere with the proper working of the Portal or any transaction being conducted on the Portal, or with any other person's use of the Portal.
- 2.7. The User shall not use the Portal or any of its content for any purpose that is unlawful or prohibited by this Agreement.

3. Data Sharing Provisions

- 3.1. The User acknowledges that the data disclosed to the User by TRAFFIC (the "**Data**"), including the personal data described at Appendix II, shall be processed strictly for the Permitted Purpose as described in this Agreement (or as otherwise agreed in writing by the Parties).
- 3.2. The Parties acknowledge that TRAFFIC is a controller of the Data it discloses to the User, and that the User will process the Data as a separate and independent controller strictly for the Permitted Purpose. In no event will the Parties process the Data as joint controllers.
- 3.3. The User shall not disseminate the Data in its raw or unaggregated form nor make it available to any third party.
- 3.4. The User shall notify TRAFFIC and await the express permission of TRAFFIC before publishing any output that makes use of the Data, and shall ensure that all resultant analyses are aggregated and the Data anonymised when used externally.
- 3.5. Each Party shall be individually and separately responsible for complying with the obligations that apply to it as a controller under Applicable Data Protection Law. In particular (and without limitation):
 - (a) TRAFFIC shall be responsible for complying with all necessary transparency and lawfulness requirements under Applicable Data Protection Law in order to disclose the Data to the User to process for the Permitted Purpose; and
 - (b) The User shall be separately and independently responsible for complying with Applicable Data Protection Law in respect of its processing of Data it receives from TRAFFIC.
- 3.6. The User will implement all appropriate technical and organisational measures, including but not limited to adequate authentication, authorisation and access control, to protect the Data (i) from accidental or unlawful destruction, and (ii) loss, alteration, unauthorised disclosure of, or access to the Data (a "**Security Incident**").
- 3.7. The User shall ensure that any person it authorises to process the Data shall be subject to statutory or contractual obligations to treat such Data as confidential.
- 3.8. The User shall have in place policies (a) that explain procedures for complying with the data protection principles of the GDPR; and (b) for retention and destruction of personal data (including timescales for such retention and destruction). On reasonable request, the User shall make these policies available to be inspected by TRAFFIC.
- 3.9. With the express written permission of TRAFFIC, the User may, at its election, appoint third party processors to process Data for the Permitted Purpose, provided that such processors: (a) agree in writing to process Data in accordance with the User's documented instructions; (b) implement appropriate technical and organisational security measures to protect the Data against a Security Incident; and (c) otherwise provide sufficient guarantees that they will process the Data in a manner that will meet the requirements of Applicable Data Protection Law.

3.10. In the event that the User receives any correspondence, enquiry or complaint from a data subject, regulator or other third party ("**Correspondence**") related to (a) the disclosure of the Data by TRAFFIC to the User; or (b) processing of Data by the User, it shall promptly inform TRAFFIC giving full details of the same, and the Parties shall cooperate reasonably and in good faith in order to respond to the Correspondence in accordance with any requirements under Applicable Data Protection Law.

4. Data Sharing outside of the EEA

4.1. The User shall not process any Data (nor permit any Data to be processed) in a territory outside of the EEA unless it has taken such measures as are necessary to ensure the transfer is in compliance with Applicable Data Protection Law.

4.2. Where the User is an organisation based outside of the EEA in a territory that has not been designated by the European Commission as an adequate level of protection, the Controller to Controller Model Clauses shall be deemed to have been completed and entered into between TRAFFIC and the User as follows:

- (a) The User will be deemed to have entered such clauses in its own name (the "data importer" in such clauses);
- (b) TRAFFIC will be deemed to have entered into such clauses in its own name (the "data exporter" in such clauses);
- (c) the provisions of Appendix II in this Agreement will be deemed to be set out in Annex B of the Controller to Controller Model Clauses;
- (d) in Clause II(h) of the Controller to Controller Model Clauses TRAFFIC and the User shall be deemed to have selected option h(iii) (the data processing principles set forth in Annex A);
- (e) the date of the Controller to Controller Model Clauses shall be deemed to be the date of this Agreement; and
- (f) to the extent that there is any conflict between the Controller to Controller Model Clauses and this Agreement, the Controller to Controller Model Clauses shall apply.

5. Acknowledgement

5.1. If the User wishes to use data from the Portal (if applicable) in any publications or reports, the User agrees to give appropriate acknowledgement to the Portal and TRAFFIC using the Portal's suggested citation or words to the same effect.

6. Duration

- 6.1. This Agreement will commence on the Effective Date and will continue in full force and effect until the termination of the last of the Data Processing Activities.

7. Miscellaneous

- 7.1. Clause headings and other headings in this Agreement are for reference only and do not constitute a part of or otherwise affect the meaning or interpretation of this Agreement.
- 7.2. The provisions of this Agreement are severable. If any phrase, clause or provision is invalid or unenforceable in whole or in part, such invalidity or unenforceability will affect only such phrase, clause or provision, and the rest of this Agreement will remain in full force and effect.
- 7.3. Any notice, letter or other communication contemplated by this Agreement will be communicated in writing via letter to the addresses set out in this Agreement, or by email to email addresses agreed between the Parties for this purpose.
- 7.4. The provisions of this Agreement will endure to the benefit of and will be binding upon the Parties and their respective successors and assigns.
- 7.5. This Agreement may be executed electronically, in counterparts, and/or via the electronic exchange of scans of fully, or partially, executed versions, each of which will be deemed an original, but all of which together will constitute one and the same instrument.
- 7.6. This Agreement (and any non-contractual dispute) shall be governed by and construed in accordance with the laws of England. The Parties submit to the exclusive jurisdiction of the courts of England and Wales to settle any dispute arising out of or in connection with this Agreement.

Appendix I

Information Sharing Protocol

Data Received by TRAFFIC

Any data received by TRAFFIC through the Portal will be recorded and stored on a system compliant with Applicable Data Protection Law. Data received will undergo an evaluation and grading process before it is used to inform decision making.

Where appropriate, with permission of the User and in line with the sharing conditions of the data, TRAFFIC may disseminate the data to relevant law enforcement agencies and appropriate non-governmental organisations. Depending on the circumstances, dissemination may include (1) specific datapoints that may contain personal data and (2) aggregated and anonymised data. These outputs can take the form of peer-reviewed reports or informed products for relevant agencies.

Information Accuracy and Retention

TRAFFIC operates a rules and convention policy whereby all recorded data is subject to review every two years. The data must meet required accuracy standards and be assessed to be justified, necessary and proportionate for retention on a database.

Disclaimer

Datasets provided by TRAFFIC on the Portal consist of information regarding wildlife trade seizures and incidents. While wildlife incident data is a vital source of information, it should not be inferred that there is a direct correlation between seizures and the overall illegal wildlife trade, or that information across locations, species or time is consistent.

TRAFFIC does not make any warranty that the Portal will be error free or that access thereto will be continuous or uninterrupted. You understand that you download from, or otherwise obtain content or services through, the Portal at your own discretion and risk. TRAFFIC cannot be held liable for any errors or inaccuracies on the Portal, or for any damage or loss caused by use of the Portal.

Any maps shown in the Portal do not imply an opinion of the legal status of borders/territories.

Appendix II

Description of the Data

Purposes of the transfer(s)

The transfer of data is made for the following purposes:

In all cases, the wildlife trade information transferred via the Portal must be used towards efforts to ensure that trade in wildlife is not a threat to the conservation of nature.

Specifically, the Portal will give the User access to TRAFFIC's open-source wildlife seizure and incident data. Relevant information and datasets may also be transferred from the User to TRAFFIC via the website, or by other means. The information will be used to increase the Parties' knowledge of illegal wildlife trade and to ensure a mutual understanding of the situation at both a national and global scale.

Data subjects

The personal data transferred may concern the following categories of data subjects:

Persons of Interest - Past, present and potential persons of interest (including accused and convicted offenders, spokespeople from related agencies, law enforcement officers, legal professionals).

Categories of data

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

Persons of Interest

- Identification data: first and last name, photograph (and other physical characteristics), date and place of birth, nationality, employment identifier, gender.
- Contact details: address, telephone number (fixed and mobile), email address, fax number, emergency contact information.
- Employment details: job title, company name, geographic location; information regarding previous roles and employment.
- Online Identifiers: Social network information; communications.
- National identifiers: national ID/passport number, tax ID; government identification number; driver's license, visa or immigration status.
- Lifestyle: history of engagement with TRAFFIC; past offences (if subject is of criminal interest); family / relationship information

Recipients

The personal data transferred may be disclosed only to the following recipients or categories of recipients:

The User; TRAFFIC.

Sensitive Data (if appropriate)

The personal data transferred may concern the following categories of sensitive data:

Ethnicity

Data Protection registration information of data exporter (where applicable):

ICO registration reference: Z757165X (TRAFFIC International Limited)