Dated 7th December 2012

AGREEMENT

[redacted]

BETWEEN

The Chief Constable of Kent Police

And

PredPol Ltd

THIS AGREEMENT made on the 7th day of December 2012 by and between

THE PARTIES

The Chief Constable of Kent ("the Chief Constable") Kent Police, Force Headquarters, Sutton Road, Maidstone, Kent ME15 9BZ and

PredPoL Ltd ("the Company") whose registered office is 5th Floor, 34 Dover Street, London W1S 4NG

A. The Parties wish to enter into a contractual relationship.

B. In connection with the contractual relationship the Parties, employees or agents of each Party may be in receipt of proprietary and confidential information.

C. In consideration of this contact the Parties agree that there will be no subcontracting or assignment of the terms agreed within this Agreement.

THE PARTIES AGREE AS FOLLOWS:

1. Purpose

1.1 The purpose of this Agreement is to deploy the Company's [redacted] predictive policing crime prediction tool within Kent Police with the aim of preventing, reducing and detecting crime and antisocial behaviour. This predictive policing approach will be used to support the Kent Police Model and explored as a sustainable tactical method designed to be effective against limited resources.

2. The Company's obligations:

2.1 To provide to the Chief Constable information following the receipt and processing of Kent Police crime and antisocial behaviour data [redacted] To provide Kent Police with daily predictive policing information, accessible [redacted] identifying key patrol locations against crime and antisocial data supplied by Kent Police.

2.2 To provide assistance with the evaluation of the impact of predictive policing in Kent with the aim of determining impact on the prevention, reduction and detection of crime and antisocial behaviour.

2.3 To provide competent personnel to process data received from the Chief Constable in order to achieve the purpose of this Agreement.

2.4 To provide adequate security systems which can be audited by the Chief Constable for the data provided.

2.5 To comply with the requirements of the Data Protection Act 1998 with due regard to full compliance for the seven principles of that Act.

2.6 The Company acknowledges and accepts it will be solely responsible for the data that it receives and will become the Data Controller in accordance with the provisions of the Data Protection Act 1998 for the data it receives from the Chief Constable.

2.7 The Company accepts full liability for any breach of data principles, the Data Protection Act 1998 and any loss attributed in relation to any such breach.

2.8 The Company will not copy, adapt, amend or translate the data to any other party without the Chief Constable's consent in writing and in any event, the data must not be transferred to any other party, subcontractor or agent of the provider.

2.9 The Company confirms and agrees that the data will remain at all times within the United Kingdom.

2.10 The Company will agree that the Chief Constable will confirm the security provision for the safe keeping of the Chief Constable's data in accordance with Schedule A and will provide access to the Chief Constable's staff for this purpose.

2.11 The Company will at all times comply with the provisions of the Data Processing Agreement set out in Schedule B which will be signed by both Parties in addition to signing of this Agreement.

2.12 The Company accepts and agrees that the data supplied by the Chief Constable is only to be used for the purpose set out in Section 1 above and is not to be used for any other purpose.

2.13 The Company agrees that the Chief Constable's data will not be placed onto any server that is shared with any other party without the written consent of the Chief Constable.

2.14 The Company agrees that it will provide to the Chief Constable 3 months written notice of the intended or forthcoming departure from it of either [redacted] or [redacted]

2.15 The Company confirms that it is the only source for this product and will hold patented rights for it.

3 The Chief Constable's Obligations

3.1 The Chief Constable will provide to the Company data [redacted]

3.2 The Chief Constable confirms that the provision of the data is for the Company to deploy its predictive policing platform for the Chief Constable.

3.3 The Chief Constable confirms that he will provide officers and staff in order to support the provision of accurate data in order that the Company can process that data accordingly.

3.4 The Chief Constable will agree to provide 7 days written notice in advance of a security visit in order to seek compliance with the security arrangements as detailed in Schedule A.

3.5 The Chief Constable accepts no liability whatsoever for the duties of the Company in relation to the data.

3.6 The Chief Constable will be able to share the outcomes of this analysis with the UK public sector agencies and partner agencies which will include but are not limited to [redacted]

4 Financial Services

4.1 The Chief Constable will pay the charges determined and agreed between the Parties.

4.2 [redacted]

4.3 [redacted]

4.4 Payment will be due 30 days from the relevant milestone set forth in Schedule C, subject to the specified retention.

5 Term of Agreement

5.1 This Agreement will commence on 10th December 2012[redacted]

6 Cancellation/Termination

6.1 This Agreement will terminate on the expiry of the time periods set forth in Schedule C, that being [redacted] unless sooner by any other clause in this Agreement.

6.2 This Agreement will terminate with immediate effect should the UK Company be placed into Receivership or Liquidation.

6.3 This Agreement will terminate if either of the Parties breach the terms of this Agreement. Such breach and intent to terminate will be provided to the other Party in writing 30 days prior to the intended termination date.

6.4 Either Party may cancel this Agreement at any time provided 90 days written notice has been given to the other Party.

7 Indemnity

7.1 Should the Chief Constable [redacted] be subject to any legal action in relation to the processing of the data or the negligence of the Company and its employees and agents, the Company will indemnify the Chief Constable [redacted] in full including all legal costs and damages.

7.2 The Company confirms that it has in place and will maintain a valid Insurance Premium to cover this Agreement and the utilisation of the Chief Constable's data to the value of [redacted] for Employer Liability, [redacted] for Public Liability and [redacted] for Professional Indemnity.

8 Parent Guarantee

8.1 The Company shall agree that it's parent Company PredPol Inc., a Californian Corporation, agrees to guarantee the performance of PredPol Ltd. The parties understand and agree that a parent guarantee is necessary and agree to draft and execute the same in good faith but in any event within 21 days following the execution of this Agreement.

9 Assignment

9.1 The Company shall not assign or otherwise transfer data provided by the Chief Constable or this Agreement.

10 Waiver

10.1 Failure or neglect by either party to enforce at any time any of the provisions hereof shall not be construed nor shall be deemed to be a waiver of that Party's rights nor in any way affect the validity of the whole or any part of this Agreement nor prejudice that Party's rights to take subsequent action.

11 Heading

11.1 The headings of this Agreement are inserted for the convenience of reference only and are not intended to be part of or to affect the meaning or interpretation of any of the terms of this Agreement.

12 Notices

12.1 Any notice to be given by either Party to the other may be sent by recorded delivery to the address as appearing herein or such other address as such Party may from time to time have communicated to the other in writing. Any notice will be deemed as served 7 days following the date of posting.

13 Breach Clause

13.1 Should the Company be found to have breached the terms of this Agreement the Chief Constable will be entitled in addition to the termination rights set out at clause 6 to recover damages as agreed by law.

14 Law

14.1 The Party's hereby agree that the Agreement concluded between them and constituted on these terms and conditions shall be construed in accordance with English law.

This Agreement is signed on the 7th day of December 2012

For and on behalf of the Chief Constable of Kent

Name.....[redacted]

Signed.....[redacted]

For and on behalf of PredPol Ltd

Name.....[redacted].....

Signed.....[redacted].....

SCHEDULE A

Information Security Requirements

Information Classification

The protective marking of data processed under this Agreement is RESTRICTED.

Confidentiality and Vetting

All personnel with access to the Chief Constables data must be listed in Schedule D along with their respective responsibilities and associated security operating procedures. All personnel will be vetted as far as is practicable.

Security Operations and Compliance

All security processes must be documented in security operating procedures. All personnel identified in Schedule D must formally sign and be issued with a copy of these procedures. Those individuals must be made aware of the importance of protecting the Chief Constable's data at all times and have received a full briefing/training session with regards to this Agreement and the associated requirements.

Non compliance and/or breaches of security arrangements will be reported to the Chief Constable's Information Security Manager and will be subject to the breach clause within the Agreement.

Physical Security of Company's processing facilities

The Company will only host and serve the Chief Constable's data from [redacted]

Storage and Access

Access to all stored data of the Chief Constable shall be restricted to the Individuals listed in Schedule D.

Secure data Disposal

At the conclusion of this Agreement if not renewed or extended the Company shall dispose of all of the Chief Constables data in the manner specified by the Chief Constable. In any event the Company cannot retain data for more than 7 years form the date of receipt of that data unless otherwise agreed in writing.

Information Security Clauses

1. Predpol will comply with the Kent Police Information Security Policy when processing its data (a copy of the policy is available from the Internet: http://www.kent.police.uk/about_us/policies/d/d01.html).
2. Kent Police data (including the predictions product) must not be moved from [redacted], without prior written authorisation from Kent Police.
3. Any changes to the Predpol service infrastructure or security procedures related to the processing of Kent Police Data must have prior written authorisation from Kent Police.
4. All infrastructure and software used to protect Kent Police information must be appropriately hardened and patched, and must also be properly configured.
5. Only personnel authorised and vetted by Kent Police will be given access to the Kent Police data (including source crime data, the predictions product, web portal, or system documentation). Predpol will provide a full access control list on request.
6. Predpol will provide a secure means of authentication for all users of the Web predictions portal. This can be based on individual user accounts or a shared account basis, as required by Kent Police. Predpol will only create portal accounts that have been authorised by Kent Police, and will provide suitable procedures for resetting passwords and reviewing and removing access rights. Predpol will enforce strong passwords that must be stored hashed/encrypted.
7. Predpol will ensure that the predictions portal can only be accessed from either the Kent Police network or Predpol's authorised network by applying suitable infrastructure boundary firewall rules.
8. Kent Police data must be stored encrypted on the predpol infrastructure and source crime data stored by Predpol must not be accessible over the Internet, once it has been securely transferred. Remote access to Kent Police source crime data must be prohibited.
9. All media used to store Kent Police information must be securely overwritten and verified to ensure that no data remains before reuse or disposal.
10. Any session that is authorised to access the Kent Police web portal must timeout, either by the application or workstation controls.
11. Predpol will not store utilities within the Kent Police Predpol environment that could be used to circumvent access controls.
12. Kent Police data must not be retained for longer than 5+2 years. This is to support the prediction accuracy requirements.
13. Predpol will not store and process any other organisations' data within the same logical network environment without prior authorisation from Kent Police.
14. Predpol will not develop or test in the production environment used to process Kent Police data and will not develop of test its products on Kent Police production data.
15. Predpol will provide written security procedures to Kent Police Information Security Manager. These must include Predpol's:
    a. management of access rights to Kent Police data, including the predictions portal;
    b. change control procedure;
    c. data retention and disposal procedure (including sanitisation of media);
    d. monitoring and audit procedure (including service availability).

16. An audit trail of all processing of Kent Police data must be maintained and made available to The Force. This includes the addition and removal of all data within the prediction process and all access (attempted and successful) via the web portal.
17. Predpol will grant Kent Police the right to audit its data processing services. Kent Police will provide at least 7 days' notice of its intention to do so.
18. Predpol will nominate a central point of contact for all information security matters. Predpol will notify the Force's Information Security Manager in the event of any actual or potential security incidents, including attempted cyber attacks of the Predpol infrastructure or applications. All evidence, including log files, will be maintained for forensic purposes.

SCHEDULE B

DATA PROCESSING AGREEMENT

THIS AGREEMENT is made the day of

BETWEEN

The Parties

The Chief Constable of Kent Police (hereinafter called the "Data Controller") of Kent Police, Force Headquarters, Sutton Road, Maidstone, Kent ME15 9BZ and *(add in third party data processor)* (hereinafter called the "Data Processor") *(add in address)* of the other part.

Purpose

The purpose of the disclosure is to facilitate the provision of predictive policing results from the company's use of data supplied in the form of crime statistical detail ("the purpose").

This Agreement sets out the terms and conditions under which Data held by the Data Controller will be disclosed to the Data Processor. This Agreement is entered into with the purpose of ensuring compliance with the Data Protection Act 1998 ("the Act"). Any processing of data must comply with the provisions of this Act.

Definitions

The following words and phrases used in this Agreement shall have the following meanings except where the context otherwise requires:

The expressions "Data", "Data Controller", "Data Processor", "Personal Data", "Sensitive Personal Data", "Processing", "Information Commissioner", have the same meaning as in Sections 1, 2 and 6 of The Data Protection Act 1998 as amended.

"Police Data" means any Data including "Personal Data" and "Sensitive Personal Data" as above provided by the Data Controller to the Data Processor and as identified in the Purpose above.

"Aggregated Data" means Police data grouped together to the extent that no living individual can be identified from that Aggregated Data or any other Data in the possession of, or likely to come into the possession of any person obtaining the Aggregated Data.

"ACPO" means the Association of Chief Police Officers.

"Government Protective Marking Scheme" means a scheme for the classification of information.

"Agreement" means this data processing agreement together with its Schedules and all other documents attached to or referred to as forming part of this agreement.

"Charges" means the amounts due and payable by the Data Controller to the Data Processor for the provision of the Services as calculated in accordance with Schedule C.

"Confidential Information" means any information relating to the Data Controller's customers and prospective customers, current or projected financial or trading situations, business plans, business strategies, developments and all other information relating to the Data Controller's business affairs including any trade secrets, know-how and any information of a confidential nature imparted by the Data Controller to the Data Processor during the term of this Agreement or coming into existence as a result of the Data Processor's obligations, whether existing in hard copy form or otherwise, and whether disclosed orally or in writing. This definition shall include all Personal Data.

Any reference to any enactment or statutory provision shall be deemed to include a reference to such enactment or statute as extended, re-enacted, consolidated, implemented or amended and to any subordinate legislation made under it; and

The word "including" shall mean including without limitation or prejudice to the generality of any description, definition, term or phrase preceding that word, and the word "include" and its derivatives shall be construed accordingly.

Information provision

It is recognised that the Purpose requires access to the data which may have been previously protectively marked by the Data Controller under the Government Protective Marking Scheme. However, that access is purely for the purpose of utilising the predictive policing tool with the aim of preventing and reducing crime and antisocial behaviour.

The Police Data will be provided over a set time period to be agreed in advance by both Parties as identified in the Agreement at section 3 (3.1).

Ownership of the Police Data shall pass to the Company and the Company will accept full liability for the data.

Use, Disclosure and Publication

The Police Data will be solely used for the purpose and no other.

Police Data will NOT be matched with any other Personal Data otherwise obtained by the Data Controller, or any other source, unless specifically authorised in writing by the Data Controller.

The Police Data will NOT be disclosed to any third party without the written authority of the Data Controller.

Access to the Police Data will be restricted to those employees of the Data Processor as listed in Schedule D and approved by the Data Controller, directly involved in the processing of the Police Data in pursuance of the Purpose.

No steps will be taken by the Data Processor to contact any Data Subject identified in the Police Data and no Police Data will be reproduced in any other format than the agreed digitalised system.

Personal Data used for research will not be published in identifiable form unless the persons concerned have given their consent and in conformity with other safeguards laid down by domestic law.

Data Protection and Human Rights

The use and disclosure of any Personal Data shall be in accordance with the obligations imposed upon the Parties to this Agreement by the Act and the Human Rights Act 1998. All relevant codes of practice or data protection operating rules adopted by the Parties will also reflect the data protection practices of each of the parties to this Agreement.

The Parties agree and declare that the information accessed pursuant to this Agreement will be used and processed with regard to the rights and freedoms enshrined within the European Convention on Human Rights. Further, the Parties agree and declare that the provision of information is proportional, having regard to the purposes of the Agreement and the steps taken in respect of maintaining a high degree of security and confidentiality.

The Parties undertake to comply with the provisions of the Act and to notify as required any particulars as may be required to the Information Commissioner.

The receipt by the Data Processor from any Data Subject of a request to access to the Data covered by this Agreement must be reported immediately to the person nominated below representing the Data Controller, who will arrange the relevant response to that request.

If any Party receives a request under the subject access provisions of the Act and personal data is identified as belonging to another Party, the receiving Party will contact the other Party to determine if the latter wishes to claim an exemption under the provisions of the Act.

It is acknowledged that where a Data Controller cannot comply with a request without disclosing information relating to another individual who can be identified from that information, he is not obliged to comply with the request, unless;

a) the other individual has consented to the disclosure of the information to the person making the request; or
b) it is reasonable in all the circumstances to comply with the request without the consent of the other individual. In determining whether it is reasonable, regard shall be had, in particular to:-

- any duty of confidentiality owed to the other individual;
- any steps taken by the data controller with a view to seeking consent of the other individual;
- whether the other individual is capable of giving consent;
- any express refusal of consent by the other individual.

If any Party receives a request for information under the provisions of the Freedom of Information Act 2000 identified as belonging to another Party, the receiving Party will contact the other Party to determine whether the latter wishes to claim an exemption under the provisions of the Act.

Where the Data Processor receives a request for information under the provisions of the Freedom of Information Act 2000 in respect of information provided by or relating to the Data Controller, the Data Processor will contact the person nominated below to ascertain whether the Data Controller wishes to claim any exemption including the determination of whether or not the Data Controller wishes to issue a response neither to confirm nor deny that information is held.

Where any Party receives a Notice under Section 10 of the Act, that Party will contact the person nominated below to ascertain whether or not to comply with that Notice.

The Data Processor shall give reasonable assistance as is necessary to the Data Controller in order to enable him to:

- Comply with request for subject access from the Data Subjects;
- Respond to Information Notices served upon him by the Information Commissioner;
- Respond to complaints from Data Subjects;
- Investigate any breach or alleged breach of the Act.

in accordance with his statutory obligations under the Act.

On reasonable notice, periodic checks may be conducted by the Data Controller to confirm compliance with this Agreement.

Confidentiality

The Data Processor shall not use or divulge or communicate to any person any Data obtained from the Data Controller, which it shall treat as private and confidential and safeguard accordingly.

The Data Processor shall ensure that any individuals involved in the Purpose and to whom Police Data is disclosed under this Agreement are aware of their responsibilities in connection with the use of that Police Data and confirmed so in writing.

For the avoidance of doubt, the obligations or the confidentiality imposed on the Parties by this Agreement shall continue in full force and effect after the expiry or termination of this Agreement.

Respect for the privacy of individuals will be afforded at all stages of the Purpose.

This clause shall not apply where disclosure of the Police Data is ordered by a Court of competent jurisdiction, or subject to any exemption under the Act, where disclosure is required by a law enforcement agency or regulatory body or Chief Constable , or if required for the purposes of legal proceedings, in which case the Data Processor shall immediately notify the Data Controller in writing of any such

requirement for disclosure of the Police Data in order to allow the Data Controller to make representations to the person or body making the requirement.

The restrictions shall cease to apply to any Data which may come into the public domain otherwise than through unauthorised disclosure by the Parties to the Agreement.

Retention, Review and Deletion

The Data Processor will dispose of Data in accordance with the requirements of Schedule A but in any event all data must be disposed after 7 years from receipt of the Data from the Data Controller.

Security

The Data Processor recognises that the Data Controller has obligations relating to the security of Data in his control under the Act, ISO7799 and the ACPO Information Community Security Policy. The Data Processor will continue to apply those relevant obligations as detailed below on behalf of the Data Controller during the term of this Agreement.

The Data Processor agrees to apply appropriate security measures, commensurate with the requirements of principle 7 of the Act to the Data, which states that "appropriate technical and organisation measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data". In particular, the Data Processor shall ensure that measures are in place to do everything reasonable to:

- make accidental compromise or damage unlikely during storage, handling, use, processing transmission or transport
- deter deliberate compromise or opportunist attack, And
- promote discretion in order to avoid authorised access

During the term of this Agreement, The Project Manager shall carry out any checks as are reasonably necessary to ensure that the above arrangements are not compromised.

The Data Controller may wish to undertake suitability checks on any persons having access to police premises and the Police data and further reserves the right to issue instructions that particular individuals shall not be able to participate in the Purpose without reasons being given for this decision. The Data Processor will ensure that each person who will participate in the Purpose understands this and provides their written consent as necessary.

The Data Processor will ensure that the personal data accessed is not used other than as identified within this agreement, and that the agreement is complied with.

The Data Controller reserves the right to undertake a review of security provided by any Data Processor and may request reasonable access during normal working hours to the Data Processor premises for this purpose. Failure to provide sufficient guarantees in respect of adequate security measures will result in the termination of this Agreement.

Access to the Police Data will be confined to authorised persons only. These will be the individual identified in the documentation attached as Schedule D.

The Data Processor undertakes not to use the services of any sub-contractors in connection with the processing of the Police Data without the prior written approval of the Data Controller.

In consideration of the provision of the Police Data for the Purpose of the Data Processor undertakes to fully indemnify and keen indemnified the Data Controller against any liability, which may be incurred by the Data Controller as a result of the Data Processor's breach of this Agreement.

Provided that this indemnity shall not apply:

a) where the liability arises from information supplied by the Data Controller which is shown to have been incomplete or incorrect, unless the Data Controller establishes that the error did not result from any wilful wrongdoing or negligence on his part
b) to the extent that the Data Controller makes any admission which may be prejudicial to the defence of the action, claim or demand.

Disputes

In the event of any dispute or difference arising between the Parties out of this Agreement, the Designated Police Manager and the Project Manager or the persons appointed pursuant to clause 9:3 of this Agreement shall meet in an effort to resolve the dispute or difference in good faith.

The Parties will, with the help of the Centre for Dispute Resolution, seek to resolve disputes between them by alternative dispute resolution. If the Parties fail to agree within 56 days of the initiation of the alternative dispute resolution procedure, then the Parties shall be at liberty to commence litigation.

Term, termination and Variation

The term of this processing agreement shall be the same as the terms of the main underlying Agreement between the Chief Constable and the Company and will automatically renew if that Agreement is renewed.

The Data Controller may at any time by notice in writing terminate this Agreement forthwith if the Data Processor is in material breach of any obligation under this Agreement.

The Data Controller will have the final decision on any proposed variation to this Agreement. No variation of the Agreement shall be effective unless it is contained in a written instrument signed by both Parties and annexed to this Agreement.

Miscellaneous

This Agreement acts in fulfilment of part of the responsibilities of the Data Controller as required by paragraphs 11 and 12 of Schedule I, Part II of the Data Protection Act 1998.

This Agreement constitutes the entire agreement between the Parties as regards the subject matter hereof and supersedes all prior oral or written agreements regarding such subject matter.

In any provision of this Agreement is held by a Court of competent jurisdiction to be invalid or unenforceable, such invalidity or unenforceability shall not affect the remaining provisions of this Agreement, which shall remain in full force and effect.

The validity, construction and interpretation of the Agreement and any determination of the performance which it requires shall be governed by the Laws of England and the Parties hereby submit to the exclusive jurisdiction of the English Courts.

Signed on behalf of the Chief Constable of Kent Police

..... Dated.....7 December 2012.

In the presence of.....

Signed on behalf of PredPol Ltd

..... Dated.....7 December 2012.

In the presence of .....

SCHEDULE C

Financial Services

REDACTED IN FULL

SCHEDULE D

List of Company representatives