DATA PROCESSING AGREEMENT

(Version 8 last revised 5 March 2021)

1. **Introduction**

1.1. This Agreement sets out the terms and conditions under which personal data held by the specified data controller will be disclosed to the specified data processor. This Agreement is entered into with the purpose of ensuring compliance with the Data Protection Act ("**Act**") 2018. Any disclosure of data must comply with the provisions of this Act.

1.2. This Agreement is made between the parties: The Chief Constables of XXXXXXXXXXXX ("**LOCALFORCE"**) of the one part and VISAV Limited (Company Registration Number: 4511143), Sherwood Business Centre, 616A – 618A Mansfield Road, Sherwood NG5 2GA ("**VISAV**").

2. Purpose

2.1. The purpose of the disclosure is to facilitate the collection and storage of membership details of members of the public/business in relation to crime initiatives for the prevention, detection and reduction of crime within specific spheres of activity (e.g. Business Crime, Neighbourhood Watch Schemes) ("the **Purpose**").

2.2. This Agreement sets out the terms and conditions under which Police Data will be processed by VISAV. The parties agree that LOCALFORCE is the Data Controller in respect of the Police Data stored on the LOCALFORCE Database. VISAV will act as a Data Controller in respect of Global Data for the purposes of administrating the VISAV Database. This Agreement is entered into with the purpose of ensuring compliance with the Act. Any processing of data must comply with the provisions of the Act.

2.3. The Purpose is consistent with the original purpose of the Police Data collection.

2.4. The Processing of the Police Data for the Purpose will assist the LOCALFORCE to fulfil his obligations to comply with the statutory duty on Chief Police Officers and relevant agencies to work together for the purpose of implementing strategies and tactics in relation to crime reduction and the prevention and detection of crime.

3. Definitions

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

3.1.1. The expressions "**Data**", "**Data Controller**", "**Data Processor**", "**Personal Data**", "**Processing**", "**Information Commissioner**", "**Data Subject**" and "**Subject Access**", have the same meaning as in Article 4 of GDPR. **Special Categories of Personal Data** has the same meaning as in Article 9 of GDPR.

3.1.2. "**System Owner**" means the organisation that commissioned and currently licences the website or other interface via which Data Subjects can register onto the VISAV Database. This may be LOCALFORCE or one of several alternative organisations such as Neighbourhood Watch, NFIB or bordering Police Forces.

3.1.3. "**Police Data**" means any Data including "Personal Data" and "Special Category Data" as above provided by the LOCALFORCE to VISAV, or provided by the Data Subject in consenting to the retention of their contact details in the VISAV Database during the process of registering or being registered where LOCALFORCE is the System Owner.

3.1.4. "**Global Data**" means any Data including "Personal Data" and "Sensitive Personal Data" provided by the Data Subject in volunteering to receive Neighbourhood Alerts and in consenting to the retention of their contact details in the VISAV Database on any website or system where LOCALFORCE is not the System Owner.

3.1.5. "**Neighbourhood Alerts**" will consist of messages and broadcasts sent to Data Subjects and Businesses that include (typically) crime alerts, appeals for witnesses to come forward, local news, awareness of public meetings, and good news stories.

3.1.6. The "**Designated Police Manager**" means the Head of Corporate Communications, on behalf of LOCALFORCE or other such person as shall be notified to VISAV from time to time.

3.1.7. The "**Project Manager**" means Mike Douglas, Director of VISAV, on behalf of VISAV, or such other person as shall be notified to LOCALFORCE from time to time.

3.1.8. "**Government Security Classification**" (GSC) means a scheme for the classification of information.

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

3.1.10. "**Confidential Information**" means any information relating to the LOCALFORCE's customers and prospective customers, current or projected financial or trading situations, business plans, business strategies, developments and all other information relating to the LOCALFORCE's business affairs including any trade secrets, know-how and any information of a confidential nature imparted by the LOCALFORCE to VISAV during the term of this Agreement or coming into existence as a result of VISAV's obligations, whether

existing in hard copy form or otherwise, and whether disclosed orally or in writing. This definition shall include all Personal Data.

3.1.11. "**VISAV Database**" means a computer-stored list of individuals (**Data Subjects**) who have consented to have their names, principal contact details and other such information which might assist them and the organisation, normally the Licensee, to which they have given consent to be so listed, to carry out its functions. This comprises the entire Neighbourhood Alert database, operated by VISAV containing both Police Data and Global Data.

3.1.12. **"Information Provider"** means any organisation represented on the Neighbourhood Alert system which can access, subject to their consent, Data Subjects on the VISAV Database.

3.2. Headings are inserted for convenience only and shall not affect the construction or interpretation of this Agreement and, unless otherwise stated, references to clauses and schedules are references to the clauses of and schedules to this Agreement.

3.3. 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

3.4. 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.

4. Information Provision

4.1. New users register via a simple user interface or website either owned by LOCALFORCE or another System Owner. During registration, users consent to the provision of their Data to LOCALFORCE. If users so consent, this Data will be stored on the LOCALFORCE Database and shall be marked as Police Data if LOCALFORCE is the System Owner or Global Data if LOCALFORCE is not the System Owner.

4.2. It is recognised that the Purpose requires access to the Police Data, which has been previously protectively marked by LOCALFORCE under the Government Security Classification.

4.3. Ownership of the Police Data shall at all times remain with LOCALFORCE.

4.4. Access to Global Data will be unconditionally granted to LOCALFORCE for the Purpose, subject to the consent of the Data Subjects. Global Data cannot be downloaded for the purposes of transfer to an alternate system and is not owned by LOCALFORCE.

4.5. Where users choose to opt in or continue to consent to the provision of their Data to an additional Information Provider, the user's contact information will be shared as Global Data under a separate Data Processing Agreement with that Information Provider. See also clause 6.2. This will not affect the original System Owner's access and ownership of the original record.

4.6. With the exception of the existing national Neighbourhood Watch organisation, represented locally by approved Associations, and the National Fraud Intelligence Bureau (NFIB), no additional Information Provider can be represented on LOCALFORCE owned websites without the express permission of LOCALFORCE.

5. **Use, Disclosure and Publication**

5.1. The Police Data will be used solely for the Purpose.

5.2. The Police Data shall not at any time be copied, broadcast or disseminated to any other third parties, except in accordance with this Agreement.

5.3. With the exception of Origins and Socio-demographic data (Mosaic, Acorn) matching, solely for the purpose of identifying representation gaps, the Police Data will NOT be matched with any other Personal Data otherwise obtained from LOCALFORCE, unless specifically authorised in writing by LOCALFORCE

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

5.5. Clauses 5.2 and 5.4 above 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 authority, or is required for the purposes of legal proceedings, in which case VISAV shall immediately notify LOCALFORCE in writing of any such requirement for disclosure of the Police Data in order to allow LOCALFORCE to make representations to the person or body making the requirement.

5.6. No steps will be taken by VISAV to contact any Data Subject identified in the Police Data, for any reason other than system updates and support, performance monitoring, service disruption notifications and to periodically remind Data Subjects who they are sharing their data with.

6. Data Protection and Human Rights

6.1. The use and disclosure of any Personal Data comprising the Police 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.

~~6.2.~~ Save where the Police Data is provided to VISAV directly by LOCALFORCE, VISAV shall be responsible for ensuring that the Data Subject has given clear consent to process their personel data for a specific purpose and will have the right to withdraw consent at any time.

6.3. 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 Purpose and the steps taken in respect of maintaining a high degree of security and confidentiality.

6.4. 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.

6.5. The receipt by VISAV from any Data Subject of a request for access to the Data covered by this Agreement, or any complaint regarding the processing or use of Personal Data, must be reported immediately to the person nominated in clause 6.10 below representing LOCALFORCE (or such other person as is notified by LOCALFORCE to VISAV from time to time), who will arrange the relevant response to that request.

6.6. If any Party receives an information rights request under Data Protection Act 2018 the receiving Party will contact the other Party to determine how the request will be progressed. If the request under the subject access provisions of the Act and personal data is identified as belonging to another Party, if the latter wishes to claim an exemption under the provisions of the Act.

6.7. 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;

6.7.1. the other individual has consented to the disclosure of the information to the person making the request; or

6.7.2. 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:-

6.7.2.1. any duty of confidentiality owed to the other individual;

6.7.2.2. any steps taken by the data controller with a view to seeking consent of the other individual;

6.7.2.3. whether the other individual is capable of giving consent;

6.7.2.4. any express refusal of consent by the other individual.

6.8. Where VISAV receives a request for information under the provisions of the Freedom of Information Act 2000 in respect of information provided by or relating to

LOCALFORCE, VISAV will contact the person nominated below to ascertain whether LOCALFORCE wishes to claim any exemption including the determination of whether or not LOCALFORCE wishes to issue a response neither to confirm nor deny that information is held.

6.9. Where any Party receives a Notice under Section 47 DPA 2018 of the Act, that Party will contact the person nominated below in clause 6.10 below (or such other person as is notified by the relevant Party in writing from time to time) and the Parties will action the request without undue delay.

6.10. The following personnel are authorised by the Parties to assume responsibility for data protection compliance, notification, security, confidentiality, audit and coordination of subject rights and Freedom of Information:

Nominated Post holder	**Organisation**
Data Protection Officers, xxxxxxx	Police
Neighbourhood Alert Product Director,	VISAV

6.11. VISAV shall give reasonable assistance as is necessary to the LOCALFORCE in order to enable LOCALFORCE to:

6.11.1. Comply with requests for subject access from the Data Subjects;

6.11.2. Comply with requests for information under the provisions of the Freedom of Information Act 2000;

6.11.3. Respond to Information Notices served upon it by the Information Commissioner;

6.11.4. Respond to complaints from Data Subjects;

6.11.5. Investigate any breach or alleged breach of the Act.

in accordance with its statutory obligations as a Data Controller under the Act.

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

7. Confidentiality

7.1. VISAV shall not use or divulge or communicate to any person (other than those whose province it is to know the same for the Purpose, or without the prior written authority of the Data Controller) any Police Data, which it shall treat as private and confidential and safeguard accordingly.

7.2. VISAV 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 have confirmed so in writing.

7.3. 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.

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

7.5. The restrictions contained in clause 7.1 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.

8. **Retention, Review and Deletion.**

8.1. The Project Manager will be responsible for ensuring the safe subsequent disposal of the Police Data as below.

8.2. Electronic copies of the data shall be securely destroyed by either physical destruction of the storage media or secure deletion using an approved CESG data cleansing product.

8.3. VISAV shall promptly comply with any request by a Data Subject to remove the Data Subject's Personal Data from the LOCALFORCE Database or the entire VISAV Database (as appropriate). Police Data shall be retained for no longer than is reasonably necessary and in any event for no longer than 3 months following removal from the LOCALFORCE Database or the VISAV Database (as appropriate).

8.4. Requests to delete Police data by LOCALFORCE under clauses in section 12, will apply to all Police Data and VISAV will promptly advise all Data Subjects marked as Global Data that LOCALFORCE is leaving the system and provide a simple unsubscription facility to enable them to request deletion as per clause 8.3.

9. Security

9.1. VISAV recognises that LOCALFORCE has obligations relating to the security of Data in his control under the Act, ISO27001 and the NPCC (formerly ACPO) Information Community Security Policy. VISAV will continue to apply those relevant obligations as detailed below on behalf of LOCALFORCE during the term of this Agreement.

9.2. VISAV agrees to apply appropriate security measures, commensurate with the requirements of Article 5 (1) principle (f) of the Act to the Police 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, VISAV shall ensure that measures are in place to do everything reasonable to:

9.2.1. make accidental compromise or damage unlikely during storage, handling, use, processing, transmission or transport

9.2.2. deter deliberate compromise or opportunist attack, and

9.2.3. promote discretion in order to avoid unauthorised access

9.3. 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 and shall inform LOCALFORCE as soon as reasonably possible if it appears that there has been any breach of clause 9.2.

9.4. LOCALFORCE may wish to undertake suitability checks on any persons having access to police premises and the Police Data in accordance with Force Vetting Policy 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.

9.5. Any security incidents, data protection breaches and newly identified vulnerabilities must be reported to the individuals identified in clause 6.10 of this Agreement as quickly as possible to enable the Data Controller to report to the ICO within the 72-hour prescribed in the Act.

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

9.7. LOCALFORCE reserves the right to undertake a review of security provided by VISAV and may request reasonable access during normal working hours to VISAV's premises for this purpose. Failure to provide sufficient guarantees in respect of adequate security measures may result in the termination of this Agreement.

9.8. Any access to the premises used to process the Police Data by maintenance or repair contractors, cleaners or other non-authorised persons must be closely supervised to ensure that there is no access to the Police Data and there is no breach of the agreed security arrangements.

VISAV 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. Any consent given by the LOCALFORCE under the provisions of this clause shall not relieve VISAV from its obligations under this agreement and VISAV shall be liable for the acts and omissions of its sub-contractors. The LOCALFORCE hereby consents to the subcontracting of data centre services by VISAV to Space Data Centres Limited. VISAV shall ensure that any sub-contractors used in connection with the processing of Police Data are, as a minimum, required under the subcontract to meet the same level of obligations as are imposed on VISAV under this Agreement.

9.9. VISAV warrants that Police Data will not be stored or transferred outside of the UK.

9.10. The Data will be delivered to VISAV in accordance with the GSC.

9.11. The parties shall ensure that Police Data is stored and transmitted in encrypted form, and shall use the best available security practices and systems applicable to the use of the Police Data.

9.12. Where VISAV or nominated subcontractor has achieved ISO27001 accreditation a copy of the certification will be provided to LOCALFORCE.

10. Indemnity

10.1. In consideration of the provision of the Police Data for the Purpose VISAV undertakes to indemnify and keep indemnified LOCALFORCE against any liability, which may be incurred by the LOCALFORCE as a result of VISAV's breach of this Agreement to the maximum value of £5,000,000.

10.2. Provided that this indemnity shall not apply:

10.2.1. where the liability arises from information supplied by LOCALFORCE which is shown to have been incomplete or incorrect, unless LOCALFORCE establishes that the error did not result from any wilful wrongdoing or negligence on its part;

10.2.2. unless the LOCALFORCE notifies the Data Processor as soon as reasonably possible of any action, claim or demand to which this indemnity applies, commits VISAV to deal with the action, claim or demand by settlement or otherwise and renders VISAV all reasonable assistance in so dealing;

10.2.3. to the extent that the LOCALFORCE makes any admission which may be prejudicial to the defence of the action, claim or demand.

10.3. The above indemnity shall have no effect on any criminal proceeding arising from any breach of the Act.

11. Disputes

11.1. 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 6.10 of this Agreement shall meet in an effort to resolve the dispute or difference in good faith.

11.2. 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 each Party shall be at liberty to commence litigation.

12. Term, Termination and Variation

12.1. This Agreement shall operate concurrently with the Alert Licence unless other wise changed by agreement.

12.2. LOCALFORCE may at any time by notice in writing terminate this Agreement forthwith if VISAV is in material breach of any obligation under this Agreement. For the avoidance of doubt, breach of clauses 5, 7, 8 or 9 of this Agreement by VISAV shall constitute a material breach.

12.3. LOCALFORCE 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.

13. Miscellaneous

13.1. This Agreement acts in fulfilment of part of the responsibilities of the Data Controller as required by Articles 28 and 29 and Recital 81 of GDPR.

13.2. If 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.

13.3. 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.

14. Lawful Basis for Processing

14.1. Under the GDPR the data processed via the system consists of:

14.1.1. Personal Data: name, address, email, telephone number processed to enable LOCALFORCE to engage with the public. Processing of personal data of individuals will be limited to those individuals who register to access the service and the lawful basis relied on is consent.

14.1.1.1. GDPR 2018 Article 6(1)- Processing shall be lawful only if and to the extent that at least one of the following applies:

14.1.1.1.1. the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

14.2. Criminal offence data: personal data of suspects collected for the Law Enforcement Purpose – messages including criminal offence data which may be released into the public domain to enable LOCALFORCE to investigate crimes and to meet the law enforcement purpose (DPA 2018 Section 31) – these messages will also be sent by email to individuals. Criminal offence data will only be processed under the authority of the senior investigations officer in order to engage with the public to gather evidence/intelligence in the specific criminal investigation.

14.3. DPA 2018 – Part 3 Section 35 (5) The second case is where:

14.3.1. the processing is strictly necessary for the law enforcement purpose,

14.3.2. the processing meets at least one of the conditions in Schedule 8, and

14.3.3. at the time when the processing is carried out, the controller has an appropriate policy document in place (see section 42).

14.4. Schedule 8 (1) statutory purposes including policing purposes as defined by MOPI 2005 and to prevent and detect crime and ASB under Crime and Disorder Act 1998

14.5. Schedule 8(3) protecting individual's vital interests

14.6. Schedule 8(4) Safeguarding of children and of individuals at risk

14.7. Schedule 8(8) Preventing fraud

14.8. LOCALFORCE have appropriate policy documents in place including a Register of Processing Activities, DP Policy and Retention Policy.

Signed on behalf of the Chief Constables of xxxxxxxxxxxxxxxx

……...……...

Date ……..…….

Signed on behalf of VISAV

……..

Date ……..…….