Pixmore Centre, Pixmore Avenue, Letchworth, SG6 1JG
+44 (0)800 158 3830 I enquiries@forensicanalytics.co.uk

DATA PROCESSING AGREEMENT

This data processing agreement ("**DPA**") forms part of the terms and conditions for the supply of products and services, and, where applicable, the end user licence agreement for the use of software (the "**Applicable Terms**") between you (the "**Customer**") and Forensic Analytics Ltd registered in England and Wales with company number 08606475 and registered address at Pixmore Centre Unit L Pixmore Centre, Pixmore Avenue, Letchworth Garden City, Hertfordshire, United Kingdom, SG6 1JG ("**Forensic Analytics**").

Any capitalised terms in this DPA which are not otherwise defined shall have the meaning given in the Applicable Terms. In the event of any conflict between any terms of the Applicable Terms and this DPA, this DPA shall take priority. The Schedule forms part of this DPA and will have effect as if set out in full in the body of this DPA. Any reference to this DPA includes the Schedule.

This DPA shall apply to the extent that Forensic Analytics Processes any Personal Data on behalf of the Customer in relation to the Services and is incorporated into the Applicable Terms by reference.

1. DEFINITIONS

1.1 In this DPA, the following terms shall have the following meanings:

"Customer Personal Data" means all Personal Data which is owned or controlled by the Customer, and which is provided by the Customer to Forensic Analytics or comes into the possession of Forensic Analytics as a result of or in connection with the supply of the Services or its obligations under the Applicable Terms;

"Data Protection Law" means applicable laws and regulations relating to the processing, privacy, and use of Personal Data, in force from time to time, including Regulation (EU) 2016/679 and the UK General Data Protection Regulation (as defined in The Data Protection Act 2018) (collectively "**GDPR**"), the Data Protection Act 2018, the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2426/2003) and any laws or regulations implementing, amending or replacing the above;

"Services" means the services to by supplied by Forensic Analytics to the Customer under the Applicable Terms; and

The terms "**Controller**", "**Data Subject**", "**Personal Data**", "**Personal Data Breach**", "**Processing**", "**Processor**" and "**Supervisory Authority**" shall have the meaning given under Data Protection Law (and "**Process**" and "**Processes**" shall be construed accordingly and references to Supervisory Authority shall include the UK Information Commissioner's Office).

2. DATA PROTECTION

2.1 To the extent that Forensic Analytics Processes any Customer Personal Data on behalf of the Customer as a Processor as a result of or in connection with Services, the parties agree that the provisions of this DPA shall apply.

2.2 The parties agree that the Customer is the Controller and Forensic Analytics is the Processor of any Customer Personal Data that Forensic Analytics Processes on behalf of the Customer in connection with the Services that is described in Schedule 1 of this DPA. Each party shall comply with its applicable obligations under Data Protection Law.

2.3 The Customer warrants and represents that it has the authority, rights, and (where applicable) consents necessary to enable Forensic Analytics to Process the Customer Personal Data in accordance with the Data Protection Law for the purposes of this DPA. The Customer shall ensure that the relevant Data Subjects have been informed of, and (if applicable) have given their consent, and that the Customer has an appropriate legal ground for the Processing of the Customer Personal Data for the purposes of this DPA as required by Data Protection Law.

2.4 The Customer shall ensure that all documented instructions to Forensic Analytics in respect of the Customer Personal Data and under this DPA shall comply with Data Protection Laws.

2.5 The parties agree that the description of Processing at Schedule 1 of this DPA is an accurate description of the Processing undertaken in relation to the Services.

2.6 Forensic Analytics will, in relation to any Customer Personal Data processed in connection with the performance Forensic Analytics of its obligations under the Applicable Terms:

2.6.1 taking into account the state of technical development and the nature of Processing, implement appropriate technical and organisational measures to protect the Customer Personal Data against accidental or unlawful destruction, loss, alteration and unauthorised disclosure or access;

2.6.2 be generally authorised by the Customer to engage with any other Processor to Process the Customer Personal Data ("**Sub-Processor**") subject to Forensic Analytics notifying the Customer of any intended changes concerning the addition or replacement of Sub-Processor(s) and permitting the Customer to object to such changes in writing within ten (10) days from the date that it is notified by Forensic Analytics. If no objection is received within such time period, the Customer shall be deemed to have given its approval to use such Sub-Processor. If the parties cannot reach agreement as to the use of a Sub-Processor, Forensic Analytics shall be entitled to terminate the applicable Services in respect of that Sub-Processor immediately by notice in writing. Forensic Analytics shall remain liable to the Customer for the acts and omissions of each Sub-processor and shall use its reasonable (but commercially prudent) endeavours to enter into a written agreement with each Sub-processor on substantially similar terms to this DPA;

2.6.3 only Process the Customer Personal Data in accordance with this DPA and the documented instructions from the Customer from time to time, unless required to do so by applicable law to which Forensic Analytics is subject; in such case, Forensic Analytics shall inform the Customer of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest. Forensic Analytics have no obligation to comply with any of the

Customer's instructions which will or are likely to (in Forensic Analytics' opinion) be inconsistent with this DPA (including the description of Processing at Schedule 1) and/or infringe Data Protection Law, and it shall promptly inform the Customer in writing of the same;

2.6.4 ensure that persons authorised to Process the Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

2.6.5 taking into account the nature of the Processing, assist the Customer, at the Customer's cost, by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests from any Data Subject for access, rectification or erasure of the Customer Personal Data, or any objection to Processing. In no event shall Forensic Analytics be obliged to respond directly to any such request unless specifically required to do so by law;

2.6.6 provide such assistance, at the Customer's cost and to the extent permitted by Data Protection Law, as the Customer reasonably requires in ensuring compliance with the Customer's obligations pursuant to Articles 32 to 36 of the UK GDPR (security of Processing, breach notification; data protection impact assessments and prior consultations) taking into account the nature of the Processing and the information available to Forensic Analytics;

2.6.7 notify the Customer without undue delay and in writing if Forensic Analytics becomes aware of a Personal Data Breach involving the Customer Personal Data, together with particulars of the breach to the extent available to Forensic Analytics;

2.6.8 at the cost of the Customer and upon reasonable notice, make available to the Customer all information that the Customer deems necessary (acting reasonably) to demonstrate compliance with the obligations laid down in this DPA and allow for and contribute to an audit (no more than once per annum) by the Customer or an auditor mandated by the Customer. In advance of such audit, the parties shall (in good faith) discuss and agree on the start date, scope and duration, and applicable security and confidentiality controls, and the Customer shall take all necessary steps to minimise the disruption to Forensic Analytics' business. Any information obtained pursuant to an audit shall be deemed to be the confidential information of Forensic Analytics;

2.6.9 only transfer Customer Personal Data outside of the United Kingdom in accordance with requirements of Data Protection Law and in accordance with the Customer's written instructions, including ensuring that there are appropriate safeguards in place in relation to the transfer, except where Forensic Analytics is required to transfer the Personal Data by the laws of the UK, member states of the

EU or EU law (and shall inform the Customer of that legal requirement before the transfer, unless those laws prevent it doing so);

2.6.10 at the option of the Customer, securely delete or return to the Customer, and delete all remaining copies of, the Customer Personal Data after the end of the provision of applicable Services relating to Processing or on termination of the Applicable Terms, whichever is sooner, unless applicable law or regulation requires storage of the Customer Personal Data;

2.6.11 allow for and contribute to audits, including inspections, conducted by the Customer or another auditor mandated by the Customer subject to the following terms:

2.6.11.1 any third-party auditor (and its directors, employees, and contractors) nominated by Customer is (i) not a competitor of Forensic Analytics; (ii) independent and free from all conflicts of interest; and (iii) in possession of appropriate professional qualifications and enters into non-disclosure agreements relating to the audit in such terms as Forensic Analytics may reasonably require;

2.6.11.2 the scope of the audit, its duration, and the times, dates and places at which it will be carried out are agreed in advance between the parties;

2.6.11.3 the Customer shall not carry out more than one audit in any rolling 12-month period; and

2.6.11.4 the Customer shall pay all (i) its own costs and expenses (including fees for the Customer's third-party auditor and its costs and expenses); and (ii) Forensic Analytics' Charges for the support of any such audit; and

2.6.12 notify the Customer if it believes that any instructions given by Customer regarding Processing infringe on the applicable Data Protection Laws and the Customer agrees that any such notice shall be made without any admission of liability by Forensic Analytics and shall not be relied on by Customer and is not technical, or legal or other professional advice.

3. LIABILITY

3.1 Each party's liability arising out of or related to this DPA, whether in contract, tort or otherwise, is subject to the limitations and exclusions of liability contained within the Applicable Terms.

4. GENERAL

4.1 This DPA shall terminate upon the expiry or termination of this Applicable Terms or, if earlier, Forensic Analytics ceasing to Process the Customer Personal Data on behalf of the Customer.

4.2 Except as set out in this DPA, the Applicable Terms shall continue in full force and effect.

Forensic Analytics
Pixmore Centre, Pixmore Avenue, Letchworth, SG6 1JG
+44 (0)800 158 3830 | enquiries@forensicanalytics.co.uk

SCHEDULE 1
DESCRIPTION OF PROCESSING

Processing of personal data (provide a description of the subject-matter and duration of the Processing):

The Customer Personal Data shall be Processed for Forensic Analytics to provide the Services. The duration of the Processing shall be the Term of the relevant agreement made under the Application Terms.

Forensic Analytics will be performing its role as a **Data Processor** on behalf of law enforcement and partner agencies. Forensic Analytics empowers investigation and intelligence teams to produce information to a robust evidential standard.

It does so through enhanced processing of digital data such as call data and handset records, downloads, ANPR, social media takeout. Maximising digital data from initial acquisition straight through to the courtroom. rapidly processing and cleansing large data sets in seconds, producing faster reports to an evidential standard accurate and actionable intelligence.

The over-arching objective of solutions provided by Forensic Analytics is to assist law enforcement and partner agencies with processing complex datasets to an evidential standard, in order too, to keep people safe, protect victims and catch criminals.

Data will be collected through user inputs and automated systems, provided by law enforcement personnel or entered the system during investigations.

For example,

- Names
- Dates of Birth
- Addresses
- Phone Numbers
- Email Addresses
- Communications Data Records (CDR)
- ANPR
- Location Data
- Health Data (as required for specific investigations, i.e. missing persons – Diabetic, Mental Health – to inform risk, this will be limited information and no access to specific health records)
- Criminal Offence Data
- Unique Identifiers (e.g., IP addresses, usernames)
- Images – (Nominals, CCTV, Screenshots)

Vehicles, communications data records, and location data may be obtained from internal lines

of business application and/or external acquisition providers.

Use:

The collected data will be used for law enforcement and partner agency purposes such as:

• Crime and intelligence analysis

• Case management

• Investigations

• Officer GPS data will be utilised for real-time tracking and coordination of law enforcement personnel.

Storage, Review, Retain and Disposal:

Data will be stored on the CSAS 360 platform within a secure Azure cloud environment with access controls and encryption to ensure confidentiality and integrity.

All data will be stored within a secure Case. Review, Retain and Disposal (RRD) configuration settings that are customisable by the Data Controller per organisation.

Data deletion will follow the RRD configuration settings, ensuring that information is securely and permanently erased when it is no longer necessary for the specified purposes.

What is the source of the data?

The sources of data include law enforcement officers, public records, databases, and other authorised channels. Officer GPS data will come from GPS-enabled devices (Mobile/Tablet devices) provided to law enforcement personnel.

Will you be sharing data with anyone?

Forensic Analytics will not be sharing any of the data it is processing to any other parties. Data may be shared with authorised personnel within the law enforcement and partner agencies for collaborative investigations and operational purposes, under the direction of the data controller (Customer).

External data sharing may occur with other law enforcement agencies, judicial bodies, or authorised third parties, following direction from the data controller, legal and privacy compliance.

External sharing could be completed manually via screenshots/Excel/PDF exports, by the data controlling organisation.

Types of processing identified as likely high risk:

• The handling of communications data records poses high risks related to privacy, collateral intrusion and security measures will be implemented to safeguard this information.

• The processing of officer GPS data involves high risk due to the sensitivity of location information. Strict access controls and encryption will be implemented to mitigate potential

risks.

• Data sharing with external entities may be considered high risk, and proper data protection agreements and safeguards will be in place to address potential risks associated with third-party involvement.

Microsoft Azure:

Data Storage and Processing: Our solution leverages Azure's capabilities to support UK law enforcement IT customers who require Police-Assured Secure Facilities (PASF) to process and store their data in the cloud. The National Policing Information Risk Management Team (NPIRMT) of the UK Home Office has completed a comprehensive security assessment of the physical infrastructure of Microsoft Azure datacenters in the UK and concluded that they're in compliance with NPIRMT requirements.

Data Encryption: Azure uses service-side encryption (SSE) to automatically encrypt your data when it is persisted to the cloud. Data in Azure Storage is encrypted and decrypted transparently using 256-bit AES encryption, one of the strongest block ciphers available, and is FIPS 140-2 compliant. Azure also provides client-side encryption for customers who need to encrypt data on the client.

Data Processing Location: Our solution ensures that your data is processed within the specified deployment region. Within the UK this will be UK West. Microsoft won't store your data outside your specified geography. Microsoft Azure is now generally available from multiple UK datacenter locations providing data residency.

Data at Rest: For data at rest, all data written to the Azure storage platform is encrypted through 256-bit AES encryption and is FIPS 140-2 compliant. This encryption is designed to prevent unauthorised access to data by ensuring the data is encrypted when on disk.

Deployment - Installation for the CSAS SaaS platform is automatic and a one-time operation via the Forensic Analytics software services team. All pre-requisites, physical infrastructure, monitoring and patching are handled through the shared responsibility model of Forensic Analytics and Microsoft Azure.

Instance - An instance refers to a single deployment of the application that serves multiple tenants. In a multi-tenant architecture, multiple tenants share a single instance of the software and its supporting infrastructure.

Tenant - A tenant often refers to a group of users, such as a customer organisation, that shares common access to and privileges within the application instance. Each tenant's data is isolated from, and invisible to, the other tenants sharing the application instance, ensuring data security and privacy for all tenants. Customer organisations control and are responsible for configuring who can access and how they are authorised to access CSAS 360 modules and services.

Example - Each customer organisation is considered a separate "tenant." In our multi-tenant architecture, all tenants share the same database instance. However, data is divided and

isolated via database schema separation, ensuring data security and privacy for all tenants. This setup allows tenants to share the same application instance while maintaining segregated data.

Data subjects

The personal data concerns the following categories of data subjects (please specify):

☒ Customer staff (past, present, and prospective)
☐ Customer customers (past, present, and prospective)
☐ Customer consultants, suppliers, contractors, subcontractors, and agents (past, present, and prospective)
☐ Customer partners (past, present, and prospective)
☐ Customer advisors (past, present, and prospective)
☐ End customer's staff (past, present, and prospective)
☐ End customer's contractors
☒ End customer's customers/end users
☒ Members of the public
☒ Children – Ages 0-18
☐ [*other - please insert*]

Purposes of the Processing

The processing is necessary for the following purposes (please specify):

The primary objectives of the processing are to enhance law enforcement and partner agencies capabilities by providing a digital forensics platform via the CSAS 360 platform. This includes improving crime and intelligence analysis, streamlining case management, and facilitating more effective investigations. The goal is to contribute to public safety and security by empowering law enforcement and partner agencies with advanced tools and insights.

The intended effect on individuals is to ensure public safety and protect the rights of citizens through more efficient and informed law enforcement and partner agency practices. By utilising the collected data, the system aims to enhance the ability to prevent and investigate criminal activities. It also seeks to improve the overall effectiveness of law enforcement efforts, contributing to a safer environment for individuals within the community.

What are the benefits of the processing:

For Law Enforcement and Partner Agencies:

- Improved efficiency in case management, intelligence and data analysis.
- Enhanced coordination and real-time tracking of personnel.
- Streamlined investigations through comprehensive data insights.
- Better resource allocation and decision-making based on a data-driven informed approach.

Public and Society:

- Increased public safety through proactive crime prevention. Intelligence and crime analysis, enhancing responses to protect those that are vulnerable and locate those that cause communities most harm.

- Timely and effective responses to incidents, investigations and emergencies.
- Improved collaboration between law enforcement and partner agencies for more comprehensive crime-solving.
- Increased public confidence in law enforcement and partner agencies that data driven coordination or resources and investigations are a responsible use of the data and information acquired.

Forensic Analytics processes data acquired directly by law enforcement and partner agencies. Our primary relationship is with law enforcement and partner agency officers and personnel, essential users of our SaaS service. Their interaction involves the acquisition of data as part of their official duties, driven by a professional and operational need essential for law enforcement and partner agency activities.

Data Collection Concerning Children and Vulnerable Groups: Data collection encompasses investigations related to (Not exhaustive):

- Missing Person Investigations
- Drug Lines
- Child Criminal Exploitation
- Child Sexual Exploitation
- Modern Slavery and Human Trafficking

These activities fall under the prevention, investigation, detection, or prosecution of criminal offences, including safeguarding against and preventing threats to public security (Part 3, s.31 DPA 2018).

- **Control and Permissions:** Law enforcement and partner agencies maintain control over the data they provide and input into our CSAS 360 SaaS service. Access controls and permissions within the system ensure that only authorised personnel can access and view cases, enhancing control over data access.
- **Handling of sensitive data, i.e. Communications Data Records (CDR):** Data, such as CDR obtained directly from network providers for crime prevention and detection, is acquired and justified separately by law enforcement and partner agencies before processing by Forensic Analytics within our CSAS 360 SaaS service.
- **Use of Organisational Employees' Data:** Given the nature of law enforcement and partner agency activities, individuals providing data, can reasonably expect its use for crime/intelligence analysis, case management, and investigative purposes, aligning with core law enforcement functions.
- **Technology Standards and Compliance**: Our technology employs state-of-the-art solutions in cloud computing, data analytics, and security protocols, compliant with industry standards. Regular updates and monitoring ensure alignment with the latest technological standards.
- **Security Measures:** No concerns or security flaws have been identified to date. Security measures, including encryption, access controls, and regular assessments,

are in place to mitigate potential risks, ensuring the confidentiality and integrity of processed data.

- **Compliance with Industry Standards**: Forensic Analytics adheres to industry standards, incorporating best practices for utilising technology to enhance crime prevention and investigation capabilities.

Forensic Analytics is certified too:

- ISO 27001 – Information Security Management Systems (ISMS)
- ISO 9001 – Quality Management Systems
- Cyber Essentials
- Cyber Essentials Plus

Industry Best Practice - Forensic Analytics are committed to industry best practice and signed up to:

- Police Cyber Alarm
- UK Police Industry Charter

Microsoft Azure (CSP) have key certifications for:

- ISO 27001 – Information Security Management Systems (ISMS)
- ISO 9001 – Quality Management Systems
- ISO 27017 **–** Information Technology – Security techniques - Information security controls.
- ISO 27018 - Protection of personal data in cloud
- ISO 27701 **–** Security techniques - Privacy information management
- Cyber Essentials Plus
- SOC 1, SOC 2, SOC 3: Service Organisation Controls for financial reporting, security, availability, processing integrity, confidentiality, and privacy
- FedRAMP: U.S. government security standards for cloud services.

Microsoft Azure ensures compliance with:

- **UK GDPR and Data Protection Act 2018**: Azure ensures compliance with the UK GDPR and the Data Protection Act 2018 by implementing robust data protection measures, including encryption, access controls, and data residency options
- **UK OFFICIAL and UK NHS Compliance**: Azure provides specific compliance offerings for UK public sector and healthcare organisations. This includes adherence to the UK Official and UK NHS regulatory standards.
- **14 Cloud Security Principles**: Azure helps customers comply with the 14 Cloud Security Principles outlined by the UK National Cyber Security Centre (NCSC). These principles cover areas such as data in transit protection, identity, authentication and secure configuration.

Public Concerns: As of now, there are no widespread public concerns related to the processing. However, we remain vigilant, acknowledging the importance of staying attuned to public sentiment and ensuring transparency in our operations to address any emerging concerns.

Pixmore Centre, Pixmore Avenue, Letchworth, SG6 1JG
+44 (0)800 158 3830 I enquiries@forensicanalytics.co.uk

Summary: The context of the processing involves a professional relationship with law enforcement and partner agency personnel, aligned with law enforcement and partner agency activities. Our commitment includes maintaining the highest standards of security and privacy, complying with industry norms, and holding certifications that validate our dedication to excellence.

Categories of data

The personal data processed fall within the following categories of data (please specify):

Identifying information and contact details

☒ Names ☒ Addresses ☒ Dates of birth ☒ Telephone numbers ☒ Time zone information ☒ Email addresses ☐ Other contact details ☒ Images ☒ Vehicle information ☒ Communications data records ☐ [*other, please insert*]

Staff information

☒ Job titles ☒ Company name ☒ Grade ☐ Demographic information ☒ Location data ☒ User ID ☐ Password ☐ [*other, please insert*]

IT system information

☒ Computer or device name / IDs ☐ Email consent ☐ Communication metadata ☒ Device IDs ☒ IP addresses, ☒CCTV ☐ [*other, please insert*]

Customer information

☒ Goods or services provided ☐ Card numbers ☐ Transaction history ☐ [*other, please insert*]

Sensitive/ special categories of data (if applicable)

The personal data processed fall within the following categories of sensitive/ special categories of data (please specify):

☒ Health information
☒ Racial or ethnic origin information
☐ Political opinion information
☒ Religious or philosophical beliefs information
☐ Trade union membership information
☐ Genetic data
☐ Biometric data
☐ Sex life or sexual orientation information
☒ Criminal conviction data
☐ N/A

Nature of Processing

The Processing by Forensic Analytics shall involve the following operations:

☒ Collection
☒ Recording
☒ Organisation
☒ Structuring
☒ Storage
☐ Adaptation or alteration
☒ Retrieval
☐ Consultation

Pixmore Centre, Pixmore Avenue, Letchworth, SG6 1JG
+44 (0)800 158 3830 I enquiries@forensicanalytics.co.uk

☒ Use ☐ Disclosure by transmission ☒ Dissemination or otherwise making available ☒ Alignment or combination ☒ Restriction ☒ Erasure or destruction ☐ [*other - please insert*]

Rights and obligations of the Controller

The rights and obligations of the Customer, as the Controller, shall be as set out in this DPA and in Data Protection Law.