Access Intelligence Security and Compliance Overview

Data privacy, protection, and security

Table of Contents

Scope

The evolving Access Intelligence portfolio includes Isentia, the market-leading media monitoring, intelligence and insights solution provider; Pulsar, an advanced social listening and audience intelligence platform; Vuelio, a leading media intelligence platform with monitoring, insight, engagement and evaluation tools; and ResponseSource, the network that connects media and influencers to the resources they need.

The products in the scope of this document are related to the following legal entities, all operating from the same physical location: The Johnson Building, 79 Hatton Garden, London, EC1N 8AW

- Access Intelligence plc
- Access Intelligence Media Comms (AIMC) trading as Vuelio
- Access Intelligence Media Data (AIMD) trading as Vuelio
- Fenix Media trading as Pulsar
- ResponseSource Ltd

Trusted Partner

All organisations should evaluate their suppliers to ensure they are happy with the levels of risk involved in any potential new partnership.

This document has been produced to assist this process by proactively explaining our stance on data protection, compliance with GDPR and our extensive work on securing client data with has resulted in ISO 27001 certification.

Any referenced certificates and policies are available to download in our Trust Centre: **https://www.accessintelligence.com/trustcentre/iso27001/**

Our brand specific privacy information is also available online:

- Pulsar Privacy Policy: https://www.pulsarplatform.com/privacy-policy/
- Vuelio & ResponseSource Privacy Policy: https://www.vuelio.com/uk/privacy-policy/

Data Protection

Authorised use of client data

All Access Intelligence products, including Pulsar Platform, Vuelio and ResponseSource, contain personal data or personally identifiable information (PII). The data subjects that this data relates to live in UK, Europe and beyond. GDPR therefore applies to this processing.

Controller and Processor relationships are a key component in GDPR. These are slightly different for each product:

- Pulsar controls the collection of data within the product. Depending on the data source, a clients search query may hit the source directly, e.g. Twitter, or indirectly via a data lake, e.g. forums. Therefore, the client is a Data Controller and Pulsar are a Data Controller.

- Vuelio/ResponseSource clients add their own private data into the product, e.g. notes, enquiries, distributions. Without this activity, we would not be processing that data. Therefore, the client is the Data Controller and Vuelio/ResponseSource are the Data Processor.

- Separately, Vuelio is the Data Controller for the collection of media/political contact data for their own purpose of building a product. Clients have access to this data and may choose to incorporate it as part of their own processing purposes, e.g. a campaign. Vuelio would still be a Data Processor in assisting clients in pursuing their own processing purposes.

The Supervisory Authority in the UK is the Information Commissioners Office (ICO). Access Intelligence does not provide legal guidance, however, to assist any organisations that may not be familiar with their legal obligations in regard to the processing of personal data, the ICO provide the following information: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-does-it-mean-if-you-are-a-controller/

Related policies:

- *ISDL13 Access Intelligence ISMS Data Protection Policy*

GDPR

The EU General Data Protection Regulation (EU GDPR) came into effect on May 25th, 2018 and reshaped the data protection laws of all 28 countries in the European Union. This affected the operating procedures and systems of all organisations which process personal data. On 31st December 2020, the UK left the EU ("Brexit") and retained EU GDPR in domestic law, but the UK now has the independence to keep the framework under review.

The UK General Data Protection Regulation (UK GDPR) is part of the new data protection landscape that includes the Data Protection Act 2018 (the DPA 2018). The UK GDPR sets out requirements for how organisations need to handle personal data. The UK GDPR applies to 'personal data', which means any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. The key principles, rights and obligations remain the same.

Access Intelligence deal with a large quantity of personal data and closely follows this legislation; as such, we are fully prepared to meet the requirements outlined within the Regulation and can demonstrate safe and secure personal data management practices across all areas of the business.

Legal Basis

Article 6 of the GDPR states that personal data processing can only take place if one (or more) of six legal bases defined within the Regulation has been established by the Data Controller. For our business, the Client is the Data Controller and Access Intelligence acts as the Data Processor by enacting their lawful, written data processing instructions. Access Intelligence will conduct data processing necessary for the Client purposes and as contracted with the Client as the Data Controller.

Vuelio & ResponseSource also maintain and provide a Media and Political Contact Database as part of the Platform and in this context, is the Data Controller, using Legitimate Interests as the legal basis for the provision of this data to Clients to communicate with these Contacts.

Data Protection Officer (DPO)

Access Intelligence has appointed a DPO who is responsible for all compliance activities. We also have appointed an EU Representative. All contact details are available in our Privacy Policies.

Records

Our DPO is responsible for the creation and maintenance of all data protection records. This includes a Record of Processing Activities (RoPA), subject access requests (SARs), Privacy Policy, risk assessments, and, where we are acting as a Data Controller, Data Protection Impact Assessments (DPIAs) and Legitimate Interest Assessments (LIAs).

Individual Rights

Data subjects (individuals), under GDPR, have several rights to the processing of their own personal data. Organisations that "control" the processing must explain to each individual how they can exercise this right and have the internal processes in place to comply within 30 days.

Subject Access Requests (SARs) are usually sent by the data subject to the data controller. The data controller would then comply with the request, which may include instructing any sub-processors (suppliers that process personal data for them) to also comply with the request.

Access Intelligence is a trusted data partner. Any SARs that our clients receive can be forwarded to gdpr@accessintelligence.com for actioning. Our processes have been externally reviewed by GDPR experts and found to comply with all requirements.

Note that by instructing Access Intelligence to action a SAR, this only applies to our scope of influence. Data Controllers will also have to action the SAR in other systems, emails, file stores etc that are outside of the influence of Access Intelligence.

Sub-Processors

Access Intelligence keeps an open record of our sub-processors in the Trust Centre: https://www.accessintelligence.com/trustcentre/sub-processors/

Any new clients must review this list before signing the contract. By signing the contract, clients are accepting our use of these sub-processors in relation to their data processing.

If Access Intelligence, or any of our brands, wish to introduce a new sub-processor, an email notification will be sent to all clients to provide a 14-day window of review.

We review all new suppliers and ensure they have sufficient information security and data protection levels. We will not partner with any supplier that increases the risk levels to our client data.

Contractual terms with suppliers will be at the same levels as we agree with our clients.

If suppliers are processing data outside of UK/EU then we will secure Standard Contractual Clauses (SCCs) with them.

Related policies:

- *ISDL19 Access Intelligence ISMS Supplier Security Management Policy*

Data Protection By Design

Our DPO regularly meets with Senior Product Managers and VPs to discuss product development plans. Compliance recommendations are included from an early stage.

Any suppliers, information assets or processes are assigned an Asset Owner. The Information Security Manager regularly reviews all information assets with Asset Owners.

This includes the processes involved in the software development life cycle.

Data Breach Notification

In any event of a data breach involving client data, we will contact all relevant data controllers (clients) within 48 hours.

The first notification email will explain the suspected or confirmed incident and outline our next steps.

Within 5 business days, there will be a detailed incident report sent to all affected clients. This will explain the number of data subjects involved, the categories of the data involved, the nature of the personal data affected as well as a summary of the incident that caused the breach and our mitigation steps.

Information Security

Prevent unauthorised access of client data

To comply with the security requirements of GDPR, Access Intelligence has developed an Information Security Management System (ISMS). The ISMS has been externally audited and achieved certification with:

- ISO 27001
- Cyber Essentials Plus

Relevant policies:

- *ISDL01 Access Intelligence ISMS Information Security Policy*

UK Cyber Essentials

Cyber Essentials is a UK government-driven initiative to promote high standards in cyber security practices across all industries and sectors.

Developed as part of the UK's National Cyber Security Programme, the UK Government worked with the Information Assurance for Small and Medium Enterprises (IASME) consortium and the Information Security Forum (ISF), to provide a clear statement of the basic controls that all organisations should implement to mitigate the risk from common internet-based threats, within the context of the Government's 10 Steps to Cyber Security.

The first stage of Cyber Essentials is a self-assessment. The second stage, or PLUS stage, is independently audited to ensure compliance.

ISO 27001

This is an international standard for Information Security Management that demonstrates an ongoing commitment to apply the most rigorous risk management model to protect information and data belonging to both Access Intelligence and its clients.

The standard forms the basis for effective management of confidential information and the application of information security controls. It recognises an ongoing commitment to review systems and suppliers, identify risks, assess implications and put controls in place for data security. This includes auditing all systems, information assets, operational processes, legal and regulatory requirements, and an ongoing training programme to strengthen the organisation's expertise in risk management and data security.

ISO 27001 recognises the Group's exceptional standards in data management and security. This benefits all clients who can rely on the company's ability to store and process sensitive data in a secure way underpinned by robust systems, increased business resilience, and improved management processes.

Accountability

Access Intelligence has assigned responsibilities for information security of Pulsar, Vuelio and ResponseSource to an Information Security Manager (ISM).

The ISM manages all security controls in the Information Security Management System (ISMS). The ISMS is internally audited at least 10 times per year and reviewed by Executive Management each month. The ISMS is also externally audited as part of our security certificates once per year.

Related policies:

- *ISDL10 Access Intelligence ISMS Roles and Responsibilities*
- *ISDL09 Access Intelligence ISMS Management Review Policy*
- *ISDL14 Access Intelligence ISMS Internal Audit Policy*

Asset Management

Information is stored in various assets and supporting assets.

Our ISMS contains a comprehensive Inventory of Assets which identifies the dedicated owner for each. Asset Owners ensure that all information assets are protected, maintaining their confidentiality, integrity, and availability.

Access to information assets is always restricted to the minimum required to undertake authorised business activities.

All assets and supporting assets are regularly reviewed. Risk Assessments are carried out based on our risk assessment methodology.

Related policies:

- *ISDL05 Access Intelligence ISMS Asset Management Policy*

Access Control

Access Intelligence has a password policy that sets out strong password requirements. If Multi-Factor Authentication (MFA) or Single Sign On (SSO) is available, then this must be enabled.

Core tools, such as Office 365 or Google Workspace, have SSO with MFA enabled.

We follow the Principle of Least Privilege. Any access or privileged access must be requested and granted by the Asset Owner.

Vuelio has password complexity rules included as standard. Client can also choose to enable:

- MFA - this will apply to all users with would involve them being send a TOTP code to their mobile phone when they login to Vuelio
- SSO – Vuelio currently supports OAuth via Azure AD

Microsoft have previously published that using MFA will block 99% of account hacks: https://www.microsoft.com/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/

Pulsar has password complexity rules included as standard. MFA is on our roadmap for 2023.

Related policies:

- *ISDL03 Access Intelligence ISMS Password Management Policy*
- *ISDL07 Access Intelligence ISMS Access Control Policy*

Workforce

All employees are screened as part of the recruitment process. All employees have confidentiality agreements and their information security responsibilities included in their job description.

Everyone at Access Intelligence understands their role and responsibilities for Information Security. These are clearly written in each policy.

Related policies:

- *ISDL53 Access Intelligence ISMS Adding Information Security Responsibilities into JD*
- *ISDL55 Access Intelligence ISMS Employee Screening Policy*

Staff Training

We have an ongoing training and education programme where all colleagues regularly refine their security and data protection knowledge.

Regular topics include: how to spot a phishing email, securing your home working environment, GDPR and what it means to you, reporting incidents etc.

To monitor staff awareness levels, we regularly send out phishing simulations and quizzes. Extra training is provided where necessary.

Any non-compliance is escalated to HR.

Relevant policies:

- *ISDL02 Access Intelligence ISMS Information Security Training Policy*

Equipment

All Access Intelligence staff have a company managed laptop. These laptops have several security controls included:

- Hard drive encryption
- User lockout after 10min of inactivity
- Password complexity rules
- Passwords change every 90 days
- Anti-Virus (AV) software
- Virtual Private Network (VPN)
- Removable media disabled
- Standard users can’t install software
- URL & email scanning
- RMM to push out weekly updates

All work must be conducted on company laptops. We do allow some work e.g. emails, to be done on smart phones that enable our local Mobile Device Management (MDM) policy.

Related policies:

- *ISDL30 Access Intelligence ISMS Mobile and Personal Device Policy*
- *ISDL16 Access Intelligence ISMS Clear Desk and Clear Screen Policy*

Physical Security

Access Intelligence is based in a contained London office. Staff have access cards to enter/exit the office. There is an occupied reception desk and all visitors must sign in and wear a visitors lanyard.

Since Q2 2020, our main street entrance has remained permanently locked. All access is now only available via the main building. This includes extra security controls of CCTV, a 24 hour security guard and secure lifts.

Please note that no client data is stored in the office. There are no local servers holding company of client data - everything is in the cloud.

There are secure rooms for networking equipment, secondary internet connections, UPS, secure cabling. All fire prevention equipment is regularly checked by a 3rd party.

Product Hosting

- Pulsar is hosted with AWS in Ireland
- Vuelio is hosted with Azure in the UK
- ResponseSource is hosted on premise in the UK

Privileged access to hosting environments and client data is monitored. MFA and SSO is enabled.

Product Development

We encourage our clients, vendors and security partners to be part of our next steps and future plans. As a result, our products are constantly improving.

All engineers are trained to be aware of common vulnerabilities such as XXS and SQL injection. Developers review the OWASP Top 10 vulnerabilities as well as guidance from NCSC and other security experts.

All source code changes are reviewed by another developers before being approved for merging into the main repository.

Quality Assurance (QA) and Product Managers (PMs) review and approve all merged changes.

A change request is then submitted for Infrastructure, Support and Security managers to review pre-production.

Pre and Post production tests e.g. regression suites are run during deployment windows.

Related policies:

- *ISDL77 Access Intelligence ISMS Secure Development Policy*
- *ISDL54 Access Intelligence ISMS Change Management Policy*

Encryption

All data in transit is encrypted with TLS1.2 (or higher).

Vuelio and ResponseSource encrypt all data at rest with AES 256-bit.

Pulsar encrypts client data at rest.

Related policies:

- *ISDL11 Access Intelligence ISMS Data Encryption Policy*

Vulnerability Management

As a SaaS provider, vulnerability identification and mitigation are crucial to our success.

The Information Security Manager works with the Infrastructure Director and Engineering Managers to ensure the following program:

- First party vulnerability scans are run on all products every month
- Third party penetration tests are run on all products every year
- Third party penetration test is run on the office every year

All identified vulnerabilities are monitored and categorised as part of the ISMS security controls. Vulnerabilities are mitigated depending on their categorisation:

- Critical = mitigated within 14 days

- High = mitigated within 30 days
- Medium = mitigated within 3 months
- Low = mitigated within 1 year

Related policies:

- *ISDL31 Access Intelligence ISMS Information Security Manual*

Patch Management

Technology is always evolving by becoming stronger, faster, smarter. It will always be tested by clients expecting high standards and malicious actors hoping for low standards.

Managing all available patches from vendors, suppliers and the tech community is crucial to our success.

The Information Security Manager works with the Infrastructure Manager and Engineering Managers and IT suppliers to ensure the following program:

- First party patches are identified every week
- Recommendations from industry leaders such as NCSC, OWASP are regularly reviewed

All identified patches are applied depending on their categorisation:

- Critical = mitigated within 14 days
- High = mitigated within 30 days
- Medium = mitigated within 3 months
- Low = mitigated within 1 year

Related policies:

- *ISDL31 Access Intelligence ISMS Information Security Manual*

Backups

Pulsar has point-in-time backups configured for 30 days. Following this there are weekly backups covering a period of 1 month. Backups are replicated to an alternative region (AWS UK) and retained for 30 days.

Vuelio have point-in-time backups configured for 7 days. Following this there are weekly backups covering a period of 1 month. Backups are replicated to an alternative region (Azure UK-West) and retained for 30 days.

Backups are immutable and require MFA to access them.

Retention

Access Intelligence has a Retention Policy to govern various processes which use client/business or personal data.

An overview:

- Pulsar client data is retained for up to 2 months after the contract has terminated
- Vuelio client data is retained for 100 days after the contract has terminated
- We will retain clients purchase records for at least 6 years

Related policies:

- *ISDL15 Access Intelligence ISMS Data Retention Policy*

Logs and monitoring

Pulsar, Vuelio and ResponseSource have been established for 10+ years and have matured logging facilities over this time to cover all common issues, incidents and debugging requirements.

Where cloud hosting is used, in-built monitoring is enabled to record who accessed/changed, what and when.

EDR software is installed on all end-points.

Products have various custom logs in place to record granular event activity. Several third-party tools have also been configured to provide extra logging and monitoring across core processes.

Business Resilience

Access Intelligence has documentation for incident management, disaster recovery and business continuity.

Disaster Recovery plans are tested at least once per year.

Pulsar has configured AWS Availability Zones to spread data across multiple separate data centres.

Vuelio has configured a second Azure Region to replicate data over 150 miles away from the primary region.

All cloud providers are ISO 27001 and SOC2 Type 2 certified. Microsoft and Amazon do not allow visitors to their data centres and are responsible for the physical security of their environments.

Related policies:

- *ISDL04 Access Intelligence ISMS Information Security Incident Management Policy*
- *ISDL08 Access Intelligence ISMS Business Continuity Policy*

Scheduled Maintenance

Access Intelligence systems undergo regular maintenance to ensure they remain in good working order. This generally does not require a system outage, however from time to time an outage is the only way the maintenance can be performed. In this case clients are given at least two day's notice.

Very infrequently, systems require urgent maintenance, with either a short notice period or no notice period at all. This only occurs if the maintenance is required to prevent further disruption.

Our standard maintenance windows are Tuesday evenings (11pm-1am)

Further Information

We are happy to assist with your review of our organisation. We pride ourselves on being transparent in our goal to be your trusted partner.

Due to the high number of requests, we ask that you share this document internally with their own supplier review teams. This should contain all the required information to complete standard review forms.

For any full policies and certificates please refer to our Trust Centre:
https://www.accessintelligence.com/trustcentre/

Thank you.

https://www.accessintelligence.com/
https://www.pulsarplatform.com/
https://www.vuelio.com/uk/
https://www.responsesource.com/