GDPR Evidence Pack

Corporate Entity

This General Data Protection Regulation Evidence Pack covers the following corporate entities: Access Intelligence, Access Intelligence Media Comms (AIMC) trading as Vuelio, Access Intelligence Media Data (AIMD) trading as Vuelio and all operating from Longbow House, 20 Chiswell Street London EC1Y 4TW.

1. Introduction to GDPR

The EU General Data Protection Regulation came into effect on May 25th, 2018 and will reshape the data protection laws of all 28 countries of the European Union (including the UK) and affect the operating procedures and systems of all organisations which process personal data. Although the United Kingdom will soon be leaving the European Union, the upcoming UK Data Protection Bill, which replaces the Data Protection Act 1998, is very close to the content of the GDPR and will bring the GDPR onto the UK statute books. Vuelio deals with a large quantity of personal data and will be directly affected by 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.

Article 5 of the Regulation sets out the principles relating to the processing of personal data: how it should be processed, for how long, which restrictions are needed, and details of the safeguards which are in place to prevent misuse. The Data Controller and Data Processor both need to demonstrate full compliance with the Regulation - to evidence this, Vuelio has prepared this document to communicate our position on the major points of the GDPR and to provide ready context for Clients interested in their own preparedness.

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 Vuelio acts as the Data Processor by enacting their lawful, written data processing instructions. Vuelio will conduct data processing necessary for the Client purposes and as contracted with the Client as the Data Controller.

Vuelio also maintains and provides 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.

2. Data Protection by Design and by Default

One of the core guiding principles of the General Data Protection Regulation is the requirement for “data protection by design and default”. Outlined in Article 25 of the Regulation, this is demonstrated through Vuelio’s commitment to implementing a framework of appropriate technical and

organisational measures which will ensure effective data protection, and only undertaking the processing of personal data that is necessary for a specific task at a given time. Technical measures include designing out any potential software or development vulnerabilities, limiting access to personal data repositories within Vuelio's platform, security and penetration testing of applications, as well as providing means for the Client to comply with their own personal data retention and disposal requirements.

3. Data Protection Impact Assessments, Risk Mitigation and the Confidentiality, Integrity and Availability of Information

Data Protection Impact Assessments (DPIA) are highlighted within the GDPR as necessary when the controlling or processing of personal data is likely to present a high risk to the rights and freedoms of a data subject. The Data Controller is required to conduct and record these assessments prior to commencing the processing of personal data, and in doing so will highlight and mitigate any risks that need to be addressed.

Vuelio have undertaken Data Protection Impact Assessments (DPIA) against all key data processing activities and these will be reviewed annually (at a minimum) to ensure that they remain current and relevant. In addition, Vuelio reviews the confidentiality, integrity and availability of all data under its control, and records those reviews in formal risk assessments which are externally validated as part of the ISO27001 certification process.

4. External Validation

Trust between Data Controllers and their selected Data Processors is of paramount importance, which is why Vuelio remains committed to demonstrating full regulatory compliance with all applicable legislation, regulations and standards.

Vuelio did previously have ISO27001:2005 certification, valid until Dec 2017. With other priorities in 2018, namely ensuring compliance with GDPR, this certification has lapsed, however the policies and processes are still in place. We are currently working towards alignment and then certification for ISO 27001:2013 – target Q1 2020. As a pre-cursor to this we achieved Cyber Essential Plus accreditation in September 2019. In addition, Vuelio use specialist external third parties to undertake regular security and penetration testing of our platform, systems and applications.

5. Data Subject Rights

A key provision of GDPR is the expansion of the rights of data subjects to access, track, correct, restrict and erase their personal data which may be in the possession of a data processing organisation.

Within the GDPR there are several significant rights afforded to data subjects that can potentially affect operations undertaken by Vuelio (as a Data Processor for the Client) and for Media and Political Contacts where Vuelio is the Data Controller. They are as follows:

- *The right of access by the data subject* – The data subject can request from the Data Controller a confirmation as to if personal data concerning them is being held. If that is the case, the data subject can then request details of the information, including the purpose of the data processing, details of where it has been disclosed, the period for which the personal data will be stored, etc.
- *The right to rectification (correction of data held)* – The data subject can obtain from the data controller the correction or completion of any inaccurate or incomplete personal data that is being held about them.
- *The right to erasure ('right to be forgotten')* – The data subject can request deletion of their personal data in certain situations, for example where the data has been processed unlawfully, is no longer needed for the purposes for which it was originally gathered, a legal obligation applies, or simply where the data subject has withdrawn their consent.
- *The right to object to processing* – The data subject can request that the data controller ceases processing of their personal data where the accuracy of the data is contested, the processing is unlawful, and where the use of the data is no longer necessary.
- *The right to restriction of processing* – The data subject can request that the data controller restricts the processing of their personal data where the accuracy of the data is contested, the processing is unlawful, and where the use of the data is no longer necessary.
- *The right to data portability* – under certain circumstances, the data subject can request an export of their personal data from the data controller directly to them, or from the controller directly to another data controller.

In each of these cases, Vuelio will be enhancing the technical functions within the to assist the applicable Data Controller (our customer) in meeting their obligations.

6. Documented Instructions provided to Vuelio

Under the GDPR, clients acting as Data Controllers must provide their Data Processors with clear documented instructions regarding the authorised processing activities for their personal data is stored within the Vuelio Platform.

Vuelio will not undertake any personal data processing activities that are not described within the Client's documented instructions. To this end Vuelio has incorporated documented instructions pertinent to our platform and delivery of services in our Terms and Conditions to aid in uniformity of processing; in contrast to holding thousands of separate (and disparate) documented instructions, we can ensure a consistent experience for clients and reduce any risk of error.

The Client must conduct any Data Protection Impact Assessments and risk assessments that are necessary in connection with the personal data processing activity, and be prepared to share the results with Vuelio if requested to demonstrate compliance.

7. Resilience, Testing and Security Controls in Place

Vuelio's main resilience objective is to ensure that we deliver our availability commitments as recorded within each Client's contracted Service Level Agreement. Vuelio operates from several segregated data centres within the UK, with our backup site and automated failover procedures designed to minimise Client service disruption in the event of a service-affecting incident. Vuelio also has an established set of business continuity scenarios mapped out and is ready to implement these if a situation so requires.

Security testing is carried out on a regular basis by internal and external teams to test aspects of operational preparedness and the management of potential risks, threats and vulnerabilities. We conduct regular penetration tests and risk assessments of our physical and digital security controls in line with the requirements of our Information Security Management System (ISMS). Vuelio maintains separate development and test environments away from its production environments, and follows secure development, testing and change control principles that are designed to prevent information security incidents. Vuelio's ISMS has been previously certified against ISO27001:2005, and Vuelio has embedded policies, processes and procedures throughout the organisation to ensure compliance with the organisation's information security and data protection requirements. Vuelio delivers a framework of regular internal audits and risk assessments to drive continuous improvement by identifying and developing all aspects of information security across the business. The controls established in the ISMS deliver a robust framework of governance and protection, not just for Vuelio, but for our Clients and any associated data subjects.

Vuelio maintains a data retention policy and supporting schedule, to make certain that personal data is only retained for as long as is necessary to carry out the specific data processing task that is required.

Vuelio provides tools within its Platform for the Client to manage their own data retention requirements. At the point at which the data is no longer needed, the data can be highlighted and securely erased, with the backups securely overwritten after 28 days. After this time, we are not able to perform any data recovery requests for our Clients.

8. Vuelio Staff, their Access and Responsibilities

Vuelio carefully select and recruit personnel to ensure the highest possible standards of professionalism and to screen any potential security risks before they could impact the business. Personnel are subject to vetting and, where applicable, police security checks. All staff are required to sign formal non-disclosure agreements as part of their on-boarding process alongside their contractual terms of employment.

Vuelio takes training and awareness regarding information security and data protection seriously. Staff are trained during their induction process on a variety of information security topics with a separate breakout session addressing GDPR compliance. Vuelio also undertakes role-specific training to cover relevant threats that may be encountered by various positions throughout the organisation, as well as running annual refresher training courses and ad-hoc sessions to address situations that have arisen and require the business's action.

Vuelio employs a principle of minimum access, such that staff are only afforded access to the data necessary and the tools required to complete the tasks required of their role. If this needs to be changed, a formal risk assessment is undertaken to decide whether a different level of access should

be granted and on what basis. Vuelio undertakes regular reviews of the access granted to all users to determine whether it is in line with their current role, as well as reviewing access and activity logs.

9. Vuelio as a Data Processor and our use of Sub-Processors

As part of Vuelio's commitment to transparency, Vuelio will disclose its use of approved sub-processors, assigning work to them within strict contractual boundaries. We will always declare any sub-processors used for a Client and we will communicate the mapping of data flow of personal information to and from them. All sub-processors are carefully selected, and are subject to ongoing checks and validations to ensure that they have GDPR-compliant information security processes and data protection practices that are no less stringent than our own.

Our contracts with such sub-processors include key clauses to ensure acceptable standards of information security and data protection. Vuelio will not contract or continue to work with any sub-processors who fail to fully comply with these. Vuelio maintains a register of Sub-Processors, available at http://www.vuelio.com/uk/Vuelio-sub-processors/.

When changing sub-processors, Vuelio will update this list not less than 4 days in advance of the date on which the change of sub-processor is effected.

10. Record Keeping

Outlined in Article 30 of the Regulation are the Record keeping responsibilities of both the Data Controller and the Data Processor. Vuelio manages Record Keeping and Retention periods for Vuelio's data and for the Data Controller's use of the Vuelio Platform. Vuelio's record keeping responsibilities include keeping records as per below:

- Client Contracts with specific Data Processing Instructions
- Supplier Contracts and Supply Chain Risk Management
- Internal and external Audit Reports
- Data Processing Impact Assessments (DPIAs)
- Software Testing Reports
- Data subject rights requests
- Privacy Policies - version controlled, and tracking
- Client service cases (including their content and status information).
- Records of ownership
- Staff training in matters of Information Security and Data Protection
- Access control information for physical locations
- Application access logs
- Data breaches, security events (real or simulated)
- Penetration testing reports and results
- External reports to relevant supervisory authorities

11. Vuelio and the Information Commissioner's Office (ICO)

Vuelio is committed to ensuring that its Clients receive the highest standard of assistance in the event of an information security incident or data breach affecting personal data. As the Data Controller in most cases, it falls to the Client to report such incidents to the Information Commissioner's Office (as the UK's supervisory authority) in a timely manner (within 72 hours of becoming aware), and communicate details of the incident to the affected data subjects. Our Data Protection Manager heads an internal team who are responsible for investigating and reporting any information security incidents, and ensures that these reports are provided to the appropriate Client promptly. Vuelio operates to an internal deadline of 24 hours from breach discovery to making a full report available to the Client. The incident report provides the following information where applicable:

- Date and time of incident, date and time of incident discovery and reporting
- Nature of incident; categorisation and description of the personal data involved
- Description of incident
- Disclosure of any data processors, sub-processors or third parties involved with the breach
- Breakdown of immediate actions and resolutions, including steps to reduce further breaches
- Root cause analysis
- Supervisory Authority notification actions undertaken
- How data subjects have been affected

12. Vuelio Data Protection Contact

As part of Vuelio's commitment to data protection and operational improvement, we have appointed a Data Protection Manager who oversees all GDPR, ISMS and information governance activities. They are the main point of contact for external parties regarding such matters and have completed formal training for the role. Their contact details are:

Andy Olliver
GDPR@vuelio.com
Vuelio Data Protection Officer
Longbow House
20 Chiswell Street
Moorgate
London
EC1Y 4TW