PULSAR*GROUP

Security, Privacy & Compliance Overview

Pulsar Group is a market leading audience intelligence business.

We deliver audience intelligence, reputation management, and marketing and communications insight for blue chip enterprises around the world.

Scope

The evolving Pulsar Group 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.

Trusted Partner

All organisations should evaluate their potential 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, information security and compliance.

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

Data Protection

Authorised use of client data

All Pulsar Group products, including Pulsar Platform, Isentia Platform, Vuelio and ResponseSource, contain personal data or personally identifiable information (PII). The Pulsar Group is committed to protecting personal data in accordance with all applicable data protection laws.

Data Protection Legislation

Personal Data is legally protected in many countries by data protection and privacy laws.

Our global privacy program is built on the world's most comprehensive data protection regulation, with the GDPR as our main guide for ensuring proper privacy practices.

By mapping GDPR principles to other regional legislations, we ensure that our practices align with the strictest requirements worldwide, providing consistent protection for all our clients and stakeholders.

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.

The UK General Data Protection Regulation (UK GDPR) is part of the new data protection landscape which includes the Data Protection Act 2018 (the DPA 2018). The UK GDPR sets out requirements for how organisations handle personal data, which includes 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 as EU GDPR.

When we refer to "GDPR" in this document, we refer to both EU GDPR and UK GDPR.

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

Controllers and Processors

The GDPR defines and distinguishes between two primary roles when it comes to collecting and processing personal data: data controllers and data processors.

A data controller determines the means and purposes for processing personal data, while a data processor is a party that processes data on behalf of the controller.

Pulsar Group is the Data Controller of:

- Any personal data relating to clients, users, website visitors, employees, job applicants
- Collecting and processing personal data during the provision of products and services

This is further explained in our Privacy Policy.

Clients are the Data Controller when:

- Processing personal data for their own purposes.
- Uploading or adding personal data to Pulsar Group products and services e.g. relationship management tools, adding notes, uploading contact records etc
- Instructing, requesting or searching whilst using Pulsar Group products and services e.g. monitoring tools, search keywords, requested reports etc

Pulsar Group entities are the Data Processor when:

- Acting on the Data Controller's behalf in the processing of personal data (as explained above)

We do so in accordance with data protection agreements agreed in our client contracts. The third-party service providers we use to help us process this data are our "sub-processors".

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.

When Pulsar Group is a Controller, our legal basis for processing Personal Data is as follows:

- **Contract** – Processing is necessary to meet contractual obligations with our clients
- **Legitimate interests** – Processing is necessary for purposes of our legitimate interests and not overridden by an individual's rights, or, our client in relation to goods and services when we process the names, contact details, job titles, and companies of our existing and prospective clients for our marketing purposes, including market research and sales leads generation; and
- **Legal obligation** – Processing is necessary to comply with a legal or administrative obligation(s).

Under the EU and UK GDPR, we process personal data based on our legitimate interests, specifically for the purpose of:

- Responding to an enquiries about our processing of an individual's Personal Data
- In response to an enquiry from individuals about our goods and services
- To promote our goods and services via direct marketing which are relevant to individuals in certain roles. We will always confirm how your Personal Data was obtained and always offer an opt-out of direct marketing communications
- The operation of our Websites (for example we collect information about usage and engagement with our Website to improve its functionality, personalisation and security)
- Communicating with individuals or our customers as necessary to provide our Services

- Our provision of products and services:
    - (i) compiling and maintaining our databases, to ensure our customers have access to the most comprehensive and up-to-date information
    - (ii) providing individuals with relevant marketing information, regular news bulletins and other information
    - (iii) referring personal information to customers of our databases: public relations and marketing professionals, public relations agencies and corporate press offices and other users of our services when individuals make an enquiry through our enquiry service
    - (iv) providing individuals with newsletters containing regular news bulletins, details regarding our products and services, latest blog content, industry news and any other information related to or otherwise connected with the above.
- Detecting or preventing illegal activities

We make sure that we check and balance any potential negative impacts on individuals before we process personal data for our legitimate interests. We do not use personal data for activities where our legitimate interests are overridden by the impact on individuals.

Supervisory Authority

A Supervisory Authority is a government-appointed body responsible for overseeing and enforcing compliance with data protection laws within a specific jurisdiction.

Where the EU GDPR applies, the supervisory authority is the EU Member State in which the client (or, if the client does not have an establishment in the EU, its representative) is established. Otherwise, if the client does not have an EU establishment or an EU representative, the Irish Data Protection Commission.

Where the UK GDPR applies, the UK Information Commissioner's Office (ICO).

Pulsar Group does not provide legal guidance, however, to assist any organisations that may not be familiar with their legal obligations as a Data Controller, 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/

Data Protection Officer (DPO)

Pulsar Group 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 Policy.

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.

Pulsar Group is a trusted data partner. Any SARs that our clients receive can be forwarded to gdpr@pulsargroup.com for attention and action. Our processes have been externally reviewed by GDPR experts and found to comply with all requirements.

Note that by instructing Pulsar Group 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 Pulsar Group.

Sub-Processors

Pulsar Group keeps an open record of our sub-processors in the Trust Centre: https://www.pulsargroup.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 Pulsar Group, or any of our brand entities, 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. Our contracts with sub-processors include key clauses to ensure acceptable standards of information security and data protection, SCCs.

Standard Contractual Clauses (SCCs)

If clients or suppliers are processing data outside of the UK/EU, we review to see if the EU has granted an "adequacy decision" for that country. If not, GDPR defines this as a "restricted transfer" as the destination country does not provide the same level of protection. To ensure that data is always protected to the same standard, we will include extra agreements in these contracts:

- Where the EU GDPR applies, the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("EU SCCs"), available here: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj
- Where the UK GDPR applies, standard data protection clauses for processors adopted pursuant to Article 46(2)(c) or (d) of the UK GDPR ("UK SCCs" / "UK Addendum"), available here: https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf

Data Protection By Design

Data privacy and security controls are embedded in our software development life cycle.

All team members receive regular privacy and security training to ensure the systems they design, build, deploy, and process personal data safely and securely.

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

Data Breach Notification

In any event of a data breach involving client data, we will contact all relevant data controllers (clients) within 24 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, Pulsar Group has developed an Information Security Management System (ISMS). The ISMS has been externally audited and achieved certification with:

- ISO 27001
- Cyber Essentials Plus

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 Pulsar Group 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

Pulsar Group 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 8 times per year and reviewed by Executive Management each month. The ISMS is also externally audited as part of our security certificates twice per year.

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.

Supplier Management

Information is stored with cloud suppliers.

New suppliers are reviewed to ensure they hold the same level of security & privacy posture that complies with Pulsar Group's Information Security Policy. After onboarding, suppliers are reviewed annually.

As well as information security and data protection & privacy, these checks also include reviewing quality, availability, and continuity of service.

Access Control

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

Pulsar Group 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.

Pulsar, Vuelio and Isentia products have password complexity rules included as standard. Client's can also choose to enable:

- MFA - this will apply to all users and will involve them being sent a SMS/TOTP code to their mobile phone when they login
- SSO – enables clients to apply their own authentication policies and user control to the products (supporting OAuth via Azure AD)

Microsoft has 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/

Workforce

Everyone at Pulsar Group is committed to the security & privacy of information.

All team members understand their responsibilities and have signed confidentiality agreements which cover client and business information.

We have an ongoing training and education programme where all colleagues regularly refine their knowledge of common cyber threats and how to identify them.

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.

Equipment

All Pulsar Group staff have a company-managed laptop. These laptops have several security controls included:

- Hard drive encryption
- User lockout after 10 min of inactivity
- Password complexity rules
- Endpoint Detection & Response software
- Anti-Virus 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 smartphones that enable our local Mobile Device Management (MDM) policy.

Physical Security

Pulsar Group 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.

Building entrances are protected by 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 parties.

Product Hosting

For resiliency, our products are hosted in a mix of cloud and on-premise environments:

- **Pulsar** is hosted on Amazon Web Services in Ireland
- **Vuelio** is hosted on Microsoft Azure in the UK
- **Isentia** is hosted on Amazon Web Services in Australia
- **ResponseSource** is hosted on-prem in the UK

These data centres provide physical security 24/7 and redundant utilities to ensure your data is safe.

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 XSS and SQL injection. Developers review the OWASP Top 10 vulnerabilities as well as guidance from NCSC, ACSC and other security experts.

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

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

All product updates, increments or changes must be formally approved.

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

Network Security

To protect data as it's transferred between your systems and ours we take a layered approach:

- All network traffic runs over HTTPS and is encrypted with TLS 1.2
- All products are protected behind Web Application Firewalls (WAF).
- All offices are physically secure and protected behind firewalls from well-known security vendors.
- All end-points have Endpoint Detection and Response (EDR) software enabled. This includes Anti-Virus/Anti-Malware and Intrusion Detection configurations.
- All security software is monitored 24/7/365 by an external SOC.

Vulnerability Management

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

The Information Security Manager works with the CTO and Senior Engineerings to ensure the following program:

- First party vulnerability scans are run on all products continuously
- 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

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 CTO, Senior Engineerings and IT suppliers to ensure the following program:

- First-party patches are identified every fortnight
- 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

Backups

Backups are immutable and require MFA to access them. Each product has it's own backup policy:

- Pulsar Platform 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 has 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.
- Isentia Platform is backed up every 24 hours. Backups are replicated to another Availability Zone.
- ResponseSource is backed up every 24 hours.

Retention

Pulsar Group 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 been terminated
- Vuelio client data is retained for 100 days after the contract has been terminated
- We will retain clients' purchase records for at least 6 years

Logs and Monitoring

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

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.

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. These logs are aggregated in a Security Information and Event Management (SIEM) solution that is monitored in real-time by an external Security Operations Centre (SOC).

Business Resilience

If Pulsar Group were ever to suspect or suffer a loss of confidentiality (e.g. data leak), integrity (e.g. website hack) or availability (e.g. service is down) the Incident Response Team would be alerted immediately. Each incident is triaged as a priority with automatic escalation configured and communicated accordingly.

Pulsar Group has documentation for incident management, disaster recovery and business continuity. Disaster Recovery plans are tested at least once per year.

Pulsar and Isentia Platforms have 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.

Scheduled Maintenance

Pulsar Group 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.

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 your teams first. This should contain all the required information to complete standard review forms.

For any further information about our organisation, products or services, please visit the relevant URL:

- https://www.pulsargroup.com/
- https://www.pulsarplatform.com/
- https://www.vuelio.com/uk/
- https://www.isentia.com/
- https://www.responsesource.com/

For any security, privacy or compliance information, including policies and certificates, please refer to our Trust Centre: https://www.pulsargroup.com/trustcentre/

Thank you.

Document Control

This document shall be reviewed annually and updated when required.

Version	Owner	Approver	Approved
2.0	Adam Palmer Head of Information Security and Privacy, DPO	Josh Lewis CTO	02/09/24

