Verified Data

Incident Response & Security Operations Summary

Overview

This document outlines the incident response and operational security practices used by Verified Data for its SaaS platforms, including:

- Verified CONSENT
- Verified ANALYTICS

The purpose of this document is to support customer assurance and vendor onboarding activities by summarising how security incidents, unintended data exposure, and operational risks are identified, contained, investigated, and remediated.

Verified Data infrastructure is hosted within Amazon Web Services (AWS) EU, primarily Ireland.

Security Principles

Verified Data operates according to the following core principles:

- Least-privilege access controls
- Encryption of data in transit and at rest
- Segregation of customer data and environments
- Continuous monitoring and logging
- Secure credential and access management
- Controlled deployment and change management processes
- Data minimisation wherever practical

Access to production systems and customer-related data is restricted to authorised personnel only.

Incident Detection

Potential incidents may be identified through:

- Automated monitoring and alerts
- Internal reviews and logging systems
- Customer or third-party reports
- Infrastructure and application monitoring
- Detection of abnormal crawler or analytics activity

Examples include:

- Unintended collection of sensitive information
- Excessive or unexpected crawler behaviour
- Unauthorised access attempts
- Third-party infrastructure or service disruption

Incident Response Process

Upon identification of a potential incident, Verified Data will:

1. Contain the issue by pausing affected services, crawler activity, or data processing where necessary
2. Restrict access to affected systems or datasets
3. Preserve relevant logs and audit information
4. Assess the scope, impact, and root cause
5. Remediate the issue and implement corrective measures
6. Notify affected customers where appropriate and proportionate

Where unintended or unnecessary data has been collected, the data will be securely deleted as soon as practical.

Verified CONSENT Controls

Verified CONSENT performs automated website auditing and crawler-based validation activities.

To minimise operational impact on customer or third-party websites, the platform implements:

- Request rate limiting
- Controlled crawler behaviour
- Monitoring of crawl activity
- Domain and path exclusions
- Manual intervention capability where required

If crawler activity unintentionally accesses sensitive information or triggers website security controls, the affected activity will be immediately suspended and reviewed.

Verified ANALYTICS Controls

Verified ANALYTICS is designed primarily as a validation and monitoring platform and does not automatically modify customer production environments.

The platform is intended to identify personally identifiable information (PII), implementation and governance-related issues while minimising unnecessary data exposure. Potential PII matches are hashed and labeled as “scrubbed” during processing. Verified Data never stores or exposes any suspected PII.

If sensitive data is unintentionally identified within analytics payloads, tags, URLs, or integrations, Verified Data will:

- Restrict access to the affected information
- Assess the scope and sensitivity of the exposure
- Securely delete unnecessary data
- Notify the customer where material risk may exist

Third-Party Infrastructure and Providers

Verified Data relies on established cloud infrastructure and supporting service providers, including AWS.

If a third-party provider experiences a material security or availability incident, Verified Data will:

- Assess potential customer impact
- Implement mitigation measures where feasible
- Monitor remediation progress
- Communicate relevant service impacts where appropriate

Business Continuity and Recovery

Verified Data maintains operational procedures intended to support service continuity and recovery, including:

- Cloud infrastructure redundancy
- Backup and recovery procedures
- Monitoring of platform availability and service health
- Controlled deployment and rollback processes

Recovery priorities focus on:

1. Protecting customer data
2. Restoring secure operations
3. Preventing recurrence

Continuous Improvement

All material incidents are reviewed internally to identify:

- Root cause
- Required operational or security improvements
- Preventive measures
- Process or monitoring enhancements

Lessons learned are incorporated into ongoing operational and security practices.

Contact

Security or incident-related enquiries: security@verified-data.com

Additional security information: verified-data.com/security