Resolver Data - Service Definition

Service overview

Resolver Data is a cloud-based analytics service providing access to anonymised, aggregated consumer complaint data. The service enables organisations to benchmark performance, identify trends, and gain insight into complaint handling and customer experience across a wide range of sectors. Resolver Data is delivered through secure, interactive dashboards and reports accessed via a web browser.

The service is designed for organisations seeking insight and benchmarking rather than operational complaint handling.

Service functionality

Resolver Data provides:

- Access to anonymised, aggregated consumer complaint datasets
- Interactive dashboards for trend analysis and benchmarking
- Filtering by issue type, category, and time period
- Comparative views across complaint themes and volumes
- Read-only access to curated datasets
- Data export for offline analysis

Buyers cannot upload, amend, or modify data within the service.

Hosting and infrastructure

- Delivered using Tableau Cloud
- Public cloud deployment
- Hosted in the United Kingdom
- No on-premises deployment
- No private cloud deployment

Physical infrastructure and datacentre operations are managed by the platform provider and its underlying cloud infrastructure provider.

Availability and resilience

Resolver Data is delivered using a highly available cloud analytics platform. The service is provided on a best-endeavours basis and does not include a formal availability SLA or service credits.

Resilience is provided through the underlying cloud platform, including redundancy and fault-tolerant design. Planned maintenance may affect availability and is communicated where possible.

Backup, restore and disaster recovery

Platform-level backup, recovery, and disaster recovery arrangements are managed by the underlying cloud and analytics platform provider. Resolver does not operate or manage physical backup infrastructure directly.

Further technical details on platform recovery arrangements are available from the platform provider on request.

Security

Resolver Data applies proportionate security controls appropriate to a read-only analytics service, including:

- Encryption in transit using TLS 1.2 or above
- Platform-managed encryption at rest
- Role-based access controls
- Multi-factor authentication for user access
- Restricted administrative access
- Platform-level security monitoring and incident handling

Physical datacentre security, penetration testing, and infrastructure security controls are managed by the platform provider and its cloud infrastructure provider.

Data protection and privacy

The service provides access to anonymised, aggregated datasets owned by Resolver. The service does not store buyer-submitted data.

Users may export data during the contract term for internal analysis. Exported data is outside the service environment and is not managed or supported by the supplier. Access to the service ends at contract termination.

Onboarding

Users are onboarded through account setup and access provisioning by Resolver. Basic guidance is provided to support access to dashboards, filtering, and data export.

No onsite training is provided as standard. Additional remote walkthroughs or guidance may be provided by agreement.

Offboarding and exit management

At contract end:

- User access to the service is removed
- Buyers retain any data exported during the contract term
- No ongoing access is provided after termination

Optional offboarding assistance beyond standard access removal may be provided by agreement and may incur additional cost.

Data access and portability

The service does not store customer-owned data. Users may export anonymised, aggregated datasets during the contract term using standard export functionality.

Supported export formats include CSV.

API access

No API access is provided.

Service constraints

- Internet access required
- Modern web browser required
- Read-only access to supplier-provided datasets
- No support for user data uploads
- Planned maintenance may affect availability

Support and service management

- Email or ticket-based support
- UK business hours support
- Support covers access and availability issues
- No dedicated account manager provided as standard
- No phone or web chat support
- Optional onsite or enhanced support by agreement

Monitoring and outage management

Service availability issues are communicated through platform-level status updates provided by the analytics platform provider. Where appropriate, users may also be notified by email. No service-specific outage reporting API is provided.

Technical requirements

Supported browsers include:

- Chrome
- Edge

- Firefox
- Safari

Recent versions only.

Compliance and governance

- Board-level responsibility for service security
- Documented information security policies and procedures
- Supplier-defined operational and security controls
- Reliance on certified third-party platform security assurances

Resolver is not currently certified to a formal information security standard.

Document control

This service definition describes the Resolver Data service as provided by Resolver Group Ltd. It may be updated periodically to reflect service changes.