CHAMELEON
DIGITAL MEDIA

Ensuring the Security of Data on Amazon AWS:

A Case Study of Datalytica

In today's rapidly evolving digital landscape, data security and compliance are paramount for organizations entrusted with sensitive information. With the increasing reliance on cloud infrastructure, it is critical that companies not only store their data securely but also ensure that their tools and platforms meet both national and international compliance standards. This paper explores the security framework of our data tool, Datalytica, which leverages Amazon AWS for data storage. We will outline how Datalytica complies with Canadian and global standards for data storage and access, as well as the internal policies that limit access to teams authorized by our senior staff and our agency of record.

Security of Data on Amazon AWS

Amazon Web Services (AWS) is widely regarded as one of the most secure cloud infrastructure platforms in the world. It adheres to the highest industry standards for data protection, offering robust encryption both in transit and at rest, identity and access management, and multi-factor authentication. AWS is certified under numerous global compliance frameworks such as ISO 27001, SOC 1, 2, and 3, and is fully compliant with the General Data Protection Regulation (GDPR) for European data protection and the Personal Information Protection and Electronic Documents Act (PIPEDA) for Canadian data protection.

Datalytica’s data is stored on AWS servers located within compliant regions to ensure adherence to data residency requirements, specifically for Canadian customers. By leveraging AWS’s security and compliance infrastructure, Datalytica ensures that our clients’ data is stored in a secure environment that is continually monitored for potential threats and vulnerabilities.

Data is encrypted within the Redshift environment using AES-256 encryption for data at rest and SSL/TLS for data in transit. Data is backed up regularly, with backups encrypted and stored securely, ensuring data integrity and availability even in the case of a disaster. This approach mitigates risks associated with multi-tenancy, such as accidental or malicious data exposure. Even in the event of a security incident, the impact is contained within a single client's schema.

Compliance with Canadian and Global Standards

Datalytica has been designed to meet and exceed the stringent requirements of data storage and access, particularly within Canadian legal frameworks like PIPEDA, as well as globally recognized standards such as the GDPR and HIPAA for sensitive health-related data. These regulations mandate clear guidelines on data privacy, secure storage, and controlled access. Datalytica ensures that all personally identifiable information (PII) and sensitive data are encrypted, access-controlled, and that only authorized individuals can retrieve or process this data.

For compliance with PIPEDA, Datalytica follows the ten principles of fair information practices. This includes transparency around data collection and usage, consent, limiting data retention, and ensuring individuals' right to access their personal data. Internationally, Datalytica aligns with GDPR's principles of data minimization, lawful processing, and maintaining secure processing environments.

Access Control and Team Security

To further safeguard sensitive data, access within Datalytica is strictly limited based on roles and responsibilities. Only teams that have been explicitly created by our senior staff, in collaboration with our agency of record, are granted access to specific data sets. These access levels are defined based on the principle of least privilege, ensuring that users only have the minimum access necessary to perform their duties.

The granularity of the access controls allows for fine-tuned permissions at various levels (e.g., report level, dataset level). This ensures that only authorized users within a client organization can access specific data or reports, minimizing the risk of unauthorized access.

Auditing mechanisms log access to data and reports, providing a traceable history of user activity, which is crucial for both security monitoring and compliance purposes.

Datalytica employs Amazon's Identity and Access Management (IAM) capabilities to enforce multi-level access controls. Through IAM policies, we can create specific roles for data scientists, analysts, and managers, ensuring that each team member can only access the data relevant to their work. This minimizes the risk of data breaches and unauthorized data access. All access requests and modifications to access controls are reviewed and authorized by senior management and the agency of record, ensuring consistent oversight and accountability.

Conclusion

The security of data held on our Amazon AWS servers, combined with Datalytica’s strict adherence to Canadian and global compliance standards, positions our platform as a trusted solution for organizations managing sensitive information. By employing best practices in data encryption, access control, and ongoing compliance with evolving regulations, Datalytica provides a secure and compliant environment for data storage and processing. Our internal policies ensure that only vetted and approved teams can access data, further mitigating risks and ensuring that the data remains protected at every stage.