ACCELARIO

Data Privacy & Security

Why Is Data Compliance Important?

Data can be a valuable asset, especially when it contains exclusive information. This is where data privacy regulations come into play. These regulations help companies reassure the general public that doing business (i.e. sharing data) with them is safe. There are plenty of data privacy laws and standards designated for a variety of industries and for different regions around the world. It is crucial to understand which laws apply to your business and how to comply with them.

Organizations commonly believe that keeping sensitive data secure from hackers means they're automatically compliant with data privacy regulations. This is not the case.

Data security and data privacy are often used interchangeably, but there are distinct differences:

Data Security protects data from compromise by external attackers and malicious insiders.

Data Privacy governs how data is collected, shared and used.

With breaches making headlines and the emergence of new privacy laws, businesses are under pressure to protect sensitive data. Accelario ensures that data is properly secured and governed, while also empowering teams to use that data when and where they need to.

There currently exist four highly influential data privacy regulations that are commonly used in most regions of the world: GDPR, HIPAA, PCI DSS, and CCPA.

- GDPR (General Data Protection Regulation)
  Country of origin: European Union
- HIPAA (Health Insurance Portability and Accountability Act) Privacy Rule
  Country of origin: United State
- PCI DSS (Payment Card Industry Data Security Standard)
  Country of origin: International
- CCPA (California Consumer Privacy Act)
  Country of origin: California, United States

Data Privacy Regulations Compliance by Accelario

Accelario easily meets all the strict regulations requirements demanded by these organizations' standards. Accelario is already installed in many of Israel's leading financial organizations:

- Five out of eight of the leading, major banking organizations in Israel
- Two out of the three top credit cards companies
- Three out of the five enterprises insurance organizations

Following a large-scale due diligence by the security and privacy regulations teams of all these organizations, Accelario meets all regulatory requirements as well as 3rd party code review, edge-case tests and security processing.

Accelario provides a comprehensive approach to compliance that works across a broad range of regional and industry privacy regulations.

The Continuous DataOps Platform by Accelario is a closed system. It is installed on the customer's premises and is not accessible externally. All version updates are managed by the customer and are manually defined by their admin.

The Accelario Internal System is protected by Admin passwords and does not require any special adjustments; it's a 'plug-n-play' solution based on active directory authentication. Permissions are either for admin or users and are based on the admin certification level of the user.

Permission levels consist of two users with two identification process:

- **Admin**
- **User**

Permission for Golden Copy database access is granted to the admin, which is the only role capable of masking and synthesizing data. Golden Copy is encrypted and is saved at the target defined by the admin.

The admin is the only one who can manage the virtual database and reconstruction of the database as well as creating copies or erasing the virtual database.

All data is kept masked within the Golden Copy and is therefore protected.

Accelario allows masking on-the-fly while the data is being copied. In this procedure sensitive information cannot be extracted from the source file in either the conversion or in the target destination.

Accelario Continuous DataOps Platform

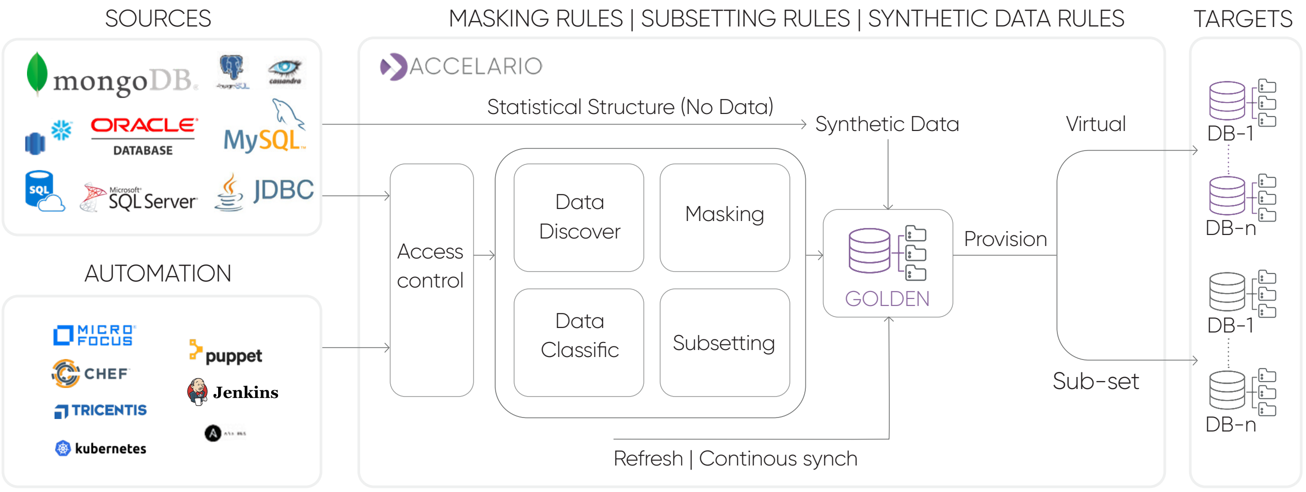
Accelario DataOps Platform offers data protection for sensitive data in a simple, one-time configuration process. Data Privacy by Accelario enables replacement of confidential information with fictitious, yet realistic data. With Accelario's automated Masking capabilities, public, private, or hybrid cloud environments can mask sensitive data values.

Masking by Accelario produces realistic values with referential integrity across disparate systems, whether on-premises or in the cloud.

Accelario DataOps Platform- Masking and Privacy capabilities, seamlessly integrates masking with data virtualization to deliver secure data to non-production targets (less secure test environments with no risk) at an accelerated pace.

- Intelligent data protection and privacy regulations
- Masking for privacy protection when migrating to cloud
- Securing privacy for test environments
- Data Compliance with New Privacy Regulations

Masking allows organizations to move data between production to less secure test environments with no risk. Protecting sensitive data in a simple, one-time configuration process. Data is masked while it is being selected, so only masked data is actually copied to the test environment.



DATA SECURITY & PRIVACY GUARNTEED FOR THE ENTIRE FLOW

To learn more about Accelario privacy and security capabilities
Read about Data Masking and Data Privacy

For more information contact us at info@accelario.com