Accelario

Accelario Data Anonymization:
Ease of Integration and Installation

Our Data Anonymization solution provides a seamless, efficient way to protect sensitive information across your organization. Accelario is designed for ease of integration and installation, ensuring that your data anonymization processes can be up and running quickly, regardless of your infrastructure. To assist with the initial setup, Accelario offers a couple of hours of free consultation to get you started, ensuring a smooth and successful implementation.

Easy Setup and Integration

Accelario makes it simple to integrate our Data Anonymization solution into your existing environment, whether it's on-premises, in the cloud on AWS, or within a Kubernetes cluster. Our straightforward installation processes and comprehensive documentation mean you can start securing your data in no time. Additionally, our support team is ready to help with any questions or issues you might encounter during setup.

On-premises

For on-premises installations, you will receive an installation kit from Accelario. The prerequisites for on-premises installation are minimal: any Windows or Linux server, with 4 CPU cores, 8GB RAM, and 100GB of disk space. The server can be a dedicated machine or the same as your database server. Once you have the kit, simply unzip it into an empty directory (referred to as "app_home") on your application server. Default configuration parameters are included but can be customized as needed. Ensure network accessibility to required databases and appropriate user privileges. To start the application, run the provided commands, and you'll be able to access the application via your browser. HTTPS setup with a self-signed certificate is included, but you can replace it with a trusted, signed certificate for enhanced security.

AWS

Start by accessing the module's AWS page and subscribing to it. Accept the terms and proceed to configure the module by filling in the necessary fields. After configuring, click continue to launch and complete the required fields. Finally, click launch, and the Accelario application will be ready to access via your browser. Simply log in to the Accelario Test Data Management Platform to start using the data anonymization solution.

Kubernetes

For Kubernetes environments, Accelario's masking application can be deployed using a Docker Hub image (accelario/masking). The application exposes port 8080 inside the container, but this can be configured to any external port via your Kubernetes infrastructure. The stateful part of the application is stored in the /work/mongo directory, and it is crucial to configure this to be stored outside of the container. For instance, you can use AWS EFS or any other type of persistent volumes. This flexibility ensures that your data remains safe and accessible even when containers are redeployed.

The Accelario Data Anonymization solution is designed to integrate effortlessly into your environment, whether on-premises, on AWS, or Kubernetes. With straightforward setup processes and robust support, Accelario ensures that you can protect your sensitive data with minimal hassle. Contact us today to benefit from our complimentary consultation and start your data anonymization journey smoothly.

About Accelario

Accelario Empowers Development Velocity With Agile Test Data Management. The dynamic needs of customers and the constant demand for new features requires faster, more agile development than ever before. Realistic testing based on accurate data is crucial — this is where Accelario shines.

Accelario empowers development teams to deliver high-quality software lightning speed by providing real, compliant, on-demand data for testing environments, all while reducing infrastructure costs. This enables rapid iterations and faster time-to-market.

Make your development process more efficient, compliant, and ready to meet today's challenges with Accelario's next-gen TDM.