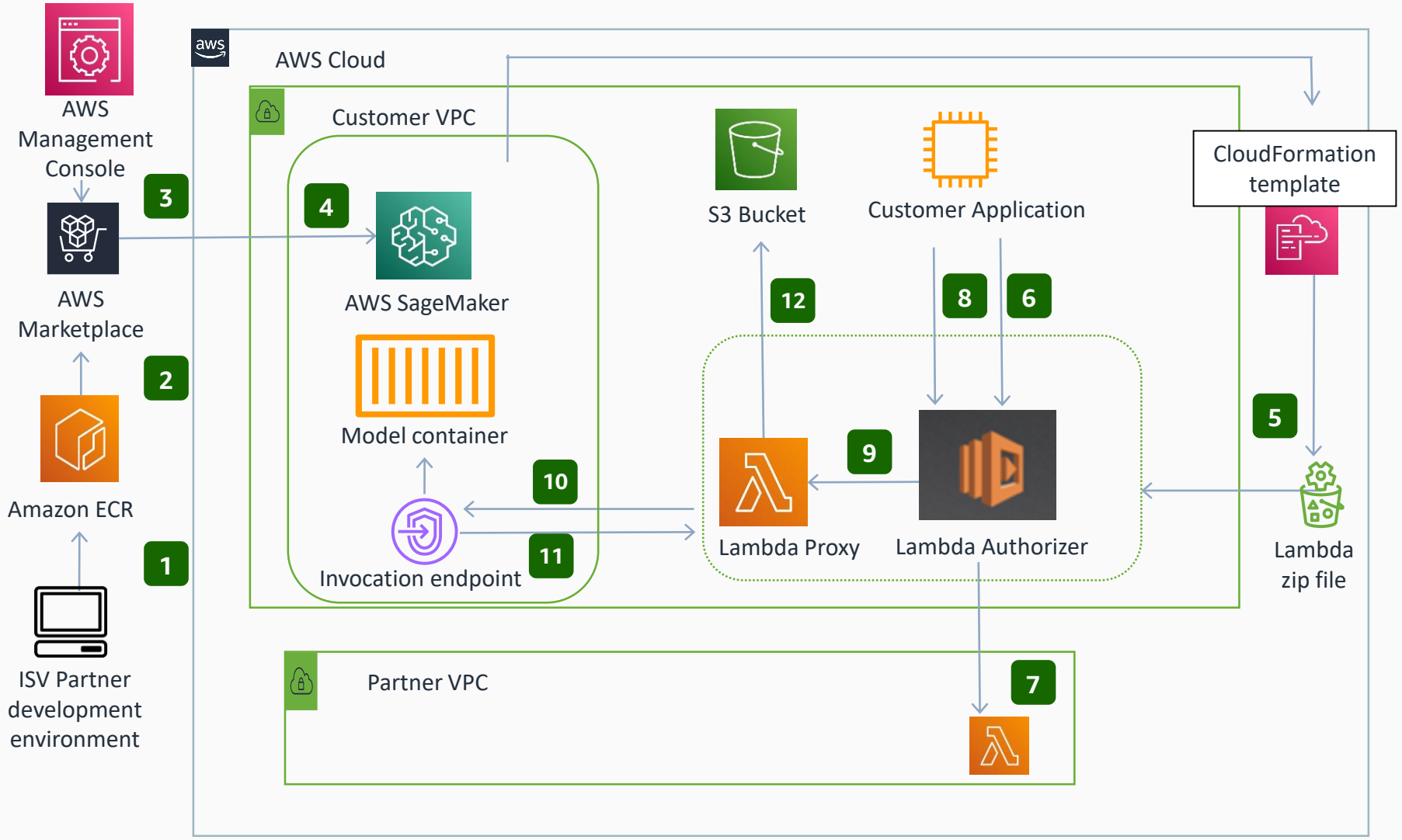
Guidance for Building Embedded Identity Services with Privacy-Safe Controls for Advertising on AWS

This architecture allows AWS customers to consume a ISV partners application in their own VPC. It is designed to protect customer's data privacy as well as partner's application implementation assets through isolated network access controls and subscription authorization.



1. ISV Partner write and package their model code as a Docker image and push the image into **Amazon Elastic Container Registry** (Amazon ECR).
2. Partner packages/pushes the image as a machine learning (ML) model for listing on AWS Marketplace.
3. Customer subscribes to the listing on AWS Marketplace.
4. Upon subscription, an **Amazon SageMaker** instance is provisioned in the customer's VPC in network isolation mode - along with the model container image and the invocation endpoint.
5. Customer runs the **AWS CloudFormation** template that deploys the **AWS Lambda** functions from the zip file located in **Amazon Simple Storage Service** (Amazon S3) repository.
6. Customer application invokes an Lambda Init endpoint to validate the subscription from the seller.
7. Lambda Authorizer then invokes the Lambda function running in partner's VPC to return an authorization token that is valid for certain duration.
8. Customer application invokes Lambda request endpoint along with authorization token and the data to be processed.
9. Lambda Authorizer validates the authorization token and forwards the call to the Lambda proxy.
10. The Lambda proxy calls the SageMaker endpoint running in network isolation mode, along with the data to be processed.
11. The SageMaker endpoint returns the response back to the Lambda function along with the processed data.
12. Lambda stores the response in the Amazon S3 bucket for the buyer application to use.