# Compliance Assessment

The General Data Protection Regulation (GPDR) is a new European privacy law, which will be enabled on May 25,2018.

It consists of several regulations regarding the organizational processing and handling of personal user data across EU regions and in the following, I will assess the compliance of my solutions architecture in regard to selected GPDR requirements for handling user data.

These requirements will be:

- Article 25: Data Protection by Design and Default (Section 1 - General Obligations)
- Article 30: Records of processing activities
- Article 32: Security of Processing
- Article 33/34: Breach Notification

## Article 25 - Data Protection by Design and Default

**Article 25** refers to technical and organisational measures "for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed." this refers to the *storage*, the *amount* and *accessibility* of the personal data being processed. Measures namely are pseudonymisation and data minimisation.

In order to comply to those requirements, the financial service company should enable several
access control mechanism allowing only authorized administrators, users and applications to have access to *customer data*. Since User data is being retrieved from the companys local data base and being processed on the cloud EC2 application server, AWS should have these mechanisms in place. They do provide the following:

- **Fine granular access** to AWS object in S3 Buckets /SQS/SNS and others
    - specifying different levels of accessibility of user data
- **Multi-factor Authentication**
- **API-Request Authentication**
    - company should make usage of IAM features to give ec2 the credentials

coming from our local data base in order to access other AWS ressources like the company application database DynamoDB

- **Geo-Restrictions**

Our Solution Architecture therefore complies to article 25.

## Article 30 - Records of processing data / Article 33, 34 - Breach Notification

*Article 30* requires that "[e]ach controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility." This means, that the processing of personal data has to be monitored.

In addition *GDPR Article 33* and *34*, breach notification has to happen within 72 hours of first having become aware of a data breach. A data breach refers to any kind of theft, loss or unauthorized access of personal data. *Data processor* who become aware of this breach are obligated to inform their data controllers and the personal users.

The companys Architecture uses *CloudWatch* for monitoring the Cloud Infrastructure. However, *CloudWatch* monitoring is designed for logging data for performance and workload factor of EC2 instances being used. This is not sufficient to comply with article 30, which requires detailled records of processing activity.

In order to comply to the mentioned articles, I hereby recommend the additional implementation of Amazon *Cloudtrail* which is a specific service to surveil governance, compliance and risks of the aws account. This service stores a history of AWS API Calls made by the AWS Management Console, the AWS SDK's and higher level AWS Services and also allows for automated trail creation and status checking of trails. Furthermore *Cloudtrail* can be easily integrated to the cloud applications using the API.

As we also set our applications server up in a VPC , which is connected to our on premise database, I recommend the usage of *VPC-FlowLogs* enabling the company to collect detailled information about flows in the network. In addition to that, the implementation of *AWS Config* allows for a detailled view and assessment of the configuration of AWS ressources.

## Article 32 Security of Processing

*Article 32* requires that organisations must implement organisational measures such as pseudonymisation and encryption of personal data.

The solution architecture store usersensible data onpremise, and uses approriate Disk and file system encryption to keep the data save. The data flow between the vpc and the local database is secured by IPsec tunnels with the VPN Gateway, therefore the company has complete control over their virtual networking environment.

Our Solution Archtiecture therefore complies to Article 32.

## Conclusion

The solution architecture made use of several technologies, which had mechanisms in place to comply to GPDR. However in order to comply to Article 30, 33, 34, the company should implement additional monitoring services such as *Cloudtrail* and *AWS Config* to keep track of configuration changes and processing activities of user data.