# HA 9 GDPR

As a company located in Germany, the legislation of the General Data Protection Regulation (GDPR) applies for us. Therefore, we have to implement some changes in our system and organisation:

## Right to Access & to be Forgotten

First of all, we have to grant out customers the right to access, whether or not personal data concerning them is being processed. Therefore, we must implement a service for customers, where they can see if we process personal data of them, and we provide copies of this data in an electronic format. This service must be free of charge. This service can easily be implemented by a microservice, which is connected to our databases. This microservice is equipped with all necessary security features, like authentication from both sides and encrypted data transfer.

This service should also include a feature for the customer, to request a Data Erasure, for granting the customer's right to be forgotten. This request will be reviewed by the controller and then executed.

## Breach Notification:

To avoid penalties, we must be able to detect data breaches as soon as possible. Thus, our CloudWatch Monitoring system will configured to alarm us, if any kind of risk for the rights and freedoms of individuals are in scope.
Moreover, we have to secure our on-premise Databases even more. They also need a Monitoring system, so we can track any kind of unauthorized access.
If these monitoring systems have detected an issue, the Data Processors have to inform the Controller, as well as our customers as soon as possible. The Messages to the Controller can be managed with intern messaging system. To notify the Customer, we need a simple automated mail transfer system. AWS Simple Email Service is perfect for this task, because of its flexible scaling possibilities and its easy integration into our existing system.

## Privacy by design:

To meet this concept, we have to redesign our data processing and data storage.
To do so, we will use pseudonymisation as soon as the customer provides us any personal information. This pseudonymisation will be encrypted and pushed through our whole life cycle so we can guarantee, that no personal data will be abused.
Also, we will only process personal data to the extent necessary for their intended purposes and should not keep it longer than necessary.

## Restoring Data:

Data restoring is an issue we have not really covered yet. Therefore, we will use an AWS Glacier to use it as a Back-up Archive. Due to its high availability and durability it is a perfect solution for our AWS Region. For the on-premise region we will have to use a different approach to store the back-ups for the customer data. Here we need at least two fully mirrored back-up servers, which are incrementally updated in the generation principle. Each generation will be stored on a tape backup in a different location as the servers are, to ensure a maximum of availability.

## DPO: Data Protection Officer:

With the new legislation, there is a need of a DPO in our company. The DPO is responsible for:

- Educating company and employees
- Training staff involved in data processing
- Monitoring the performance of our system
- Interfacing with the customer, how their data is being used and what measures we take, to protect their personal information
- Conduct audits and address potential issues
- Have an overview of the processed data and their purposes, to be able to make them public on request

## Consent:

To legally process the user there needs to be a consent between us and the customer. This means the information given by the customer must be “freely given, specific, informed and unambiguous”. To ensure this, our goal is to disclose the purposes of the customer’s data, so it is obvious what their data is going to be used for at the point of data collection.

A simple information pop-up form with a tick box to agree to our conditions should be placed at the beginning.