GDPR for ODALA - current state after front runner city deployment & Follower city status

What is GDPR?

GDPR stands for General Data Protection Regulation. It is the law governing the processing of personal data that became applicable in all EU countries in spring 2018.

The GDPR gives you more protection for your personal data and more ways to control how your data is processed.

Rights under GDPR:

Know what personal data the organisation holds about you

Know how and for what purposes your personal data is processed

Request the correction of inaccurate, inaccurate or incomplete personal data about you

Request the deletion of your personal data

Object to the processing of your personal data

Request restriction of the processing of your personal data

Transfer your data to another organisation

Not to be subject to automated decision-making without justification.

ODALA GDPR

Assessment is to be done per deployment. The platform itself is GDPR agnostic.

GDPR in Kiel and Odala deployment

The Kiel city deployment willingly collects only account information of known users; project stakeholders. The registry is formed in Keyrock. Registry consists of user’s names and email.

In addition only sensor type information is collected. No personal type information is collected, with the exception of IP adresses, which under current understanding cannot be linked to an individual.

Keyrock - an IDM

Keyrock is being used in Kiel as IDM and forms a registry. Registry contains user’s names and emails.

Keyrock is configured to ask authorization when using Oauth2. The General Data Protection Regulation (GDPR) forces clients to ask for a consent to obtain the user information. Actually, this parameter should be always true, but there are some cases in which is useful to set it to false. For instance, if a service in which existing users have already gave their consent before

and now this service wants to use Keyrock but with their own user table to authenticate those users, external authentication.

Keyrock will force the acceptance of TOS which is not defined at the time of writing.

Keycloak - an IDM

Keycloak is being used in Kiel as IDM and forms a registry. Registry contains user's names and emails.

Keycloak is configured to ask authorization when using Oauth2. The General Data Protection Regulation (GDPR) forces clients to ask for a consent to obtain the user information. Actually, this parameter should be always true, but there are some cases in which is useful to set it to false. For instance, if a service in which existing users have already gave their consent before and now this service wants to use Keyrock but with their own user table to authenticate those users(see External authentication).

Keycloak will not force the acceptance of TOS.

Mobility toolkit

The Mobility Toolkit collects information from two kinds of sources.

1. Vehicle data from traffic sensors, like traffic cameras or magnetic loop sensors. At a maximum the Mobility Toolkit collects the type of the vehicle and it's direction at this spot. No personal data is collected as well as no data which would allow for tracking of individuals is collected.
2. Optionally the Mobility Toolkit provides an integration with the OpenPath app to calibrate itself. The OpenPath app requires user consent to collect the data, GDPR compliant. It collects a transportation mode and a route of the user. This route is being anonymized by removing parts from the start and the end of the route which avoids traceability of specific users. The OpenPath app has a server component which needs to be hosted by the respective city.

The OpenPath integration is fully optional.

Environmental toolkit

The environmental toolkit displays the data collected by the sensors of the deployed IoT devices, it does not display or contain citizen data.

To add additional users, you only need a username or email, so no sensitive information is processed within the tool.

Market place

When completing an order, Market place wants users to create a My billing addresses. This collection includes email, Postal address and phone number.

In addition Marketplace collect a profile, which includes minimum of email address.

Market place has no documented GDPR compliance mechanisms in it’s documentation.

CKAN

contains the information gathered from the IoT devices connected to the ODALa ecosystem. No users information is stored in this tool, as no user logins are not allowed.

Follower city deployments

Follower cities deploy a customised version of ODALA deployment. Below is listed cities with their relevant components and their status with respect to GDPR.

Arezzo

Travel Planner

The web travel planner displays informations about public transport in the metropolitan area of Arezzo, such as bus and train stops, lines, routes, real time arrival and departures. Processing and geocoding a pair of addresses as departure and arrival points, the travel planner provides journey solutions, both with public transport (bus, train, tram etc.) and private (car walk, bike) modes. To provide these functionalities no login action is required. All informations are public accessible and no personal data is collected.

Smart City Dashboard

The Smart City Dashboard collects information about parking spot occupation, bus stops and gates for traffic-restricted zones. Data are imported and used as aggregated information for analysis purpose. No personal data is collected as well as no data which would allow for tracking of individuals.

Mobility toolkit

The Mobility Toolkit collects information from parking access sensors for vehicle tracking. Data are only used as aggregated information for analysis purpose. No personal data is collected as well as no data which would allow for tracking of individuals is collected.

Mobility Toolkit could also process data about parking occupation as time series. In this case too, no personal data as well as no data which would allow for tracking of individuals is collected.

Environmental toolkit

The environmental toolkit displays the data collected by the air quality sensors, it does not process, display or contain personal data.

Administrative users can access with username and password, with no need to provide personal data.

Saint-Quentin

Keyrock - an IDM

Keyrock is being used as IDM forms a registry. Registry contains user’s names and emails.

Keyrock is configured to ask authorization when using Oauth2. The General Data Protection Regulation (GDPR) forces clients to ask for a consent to obtain the user information. Actually, this parameter should be always true, but there are some cases in which is useful to set it to false. For instance, if a service in which existing users have already gave their consent before and now this service wants to use Keyrock but with their own user table to authenticate those users, external authentication.

Keyrock will force the acceptance of TOS which is not defined at the time of writing.

Market place

When completing an order, Market place wants users to create a My billing addresses. This collection includes email, Postal address and phone number.

In addition Marketplace collect a profile, which includes minimum of email address.

Market place has no documented GDPR compliance mechanisms in it’s documentatio

Heidelberg

On the existing UDP in Heidelberg only sensor type information is collected. No personal type information is collected, with the exception of IP adresses, which under current understanding cannot be linked to an individual.

Keycloak - an IDM

Keycloak is being used in Heidelberg as IDM and forms a registry. Registry contains user’s names and emails and is connected to the city’s Active Directory.

Keycloak is configured to ask authorization when using Oauth2. The General Data Protection Regulation (GDPR) forces clients to ask for a consent to obtain the user information.

Web Application Firewall

WAF collects IP data, which can be considered as PI information.

NGSI-LD Mapper

The NGSI-LD Mapper is a processor for Apache NIFI which transforms NGSI-V2 data to NGSI-LD in the city’s UDP. No personal type information is collected, with the exception of IP adresses, which under current understanding cannot be linked to an individual.

Cartagena

Components relevant in ODALA for GDPR:

Keycloak

Keycloak is a IDM security tools that provide authentication and authorization to all the services of the system. The tool only contains not sensible user information like email and unser name, first name, last name and environment password.

The password of the users are properly encrypted and not accessible by any other user.

Environmental toolkit

The Environmental toolkit only gatther information provided by IoT sensors about air quality and not store any other user information beyond the credential of the users able to login in the service.

CKAN

it contains the information gathered from the IoT devices connected to the ODALa ecosystem. No users information is stored in this tool.

Mobility toolkit

The environmental toolkit displays the data collected by the air quality sensors, it does not process, display or contain personal data.

Administrative users can access with username and password, with no need to provide personal data.

Other components

Other components may form a registry if used maliciously. Mechanism here is that someone willingly writes Personally Identifiable information to the platform. This is not possible with current configuration for unauthorized persons, as access control is configured so that explicit permission need to be granted by Administrator to gain write access to the platform.