#EOSHACKATHON

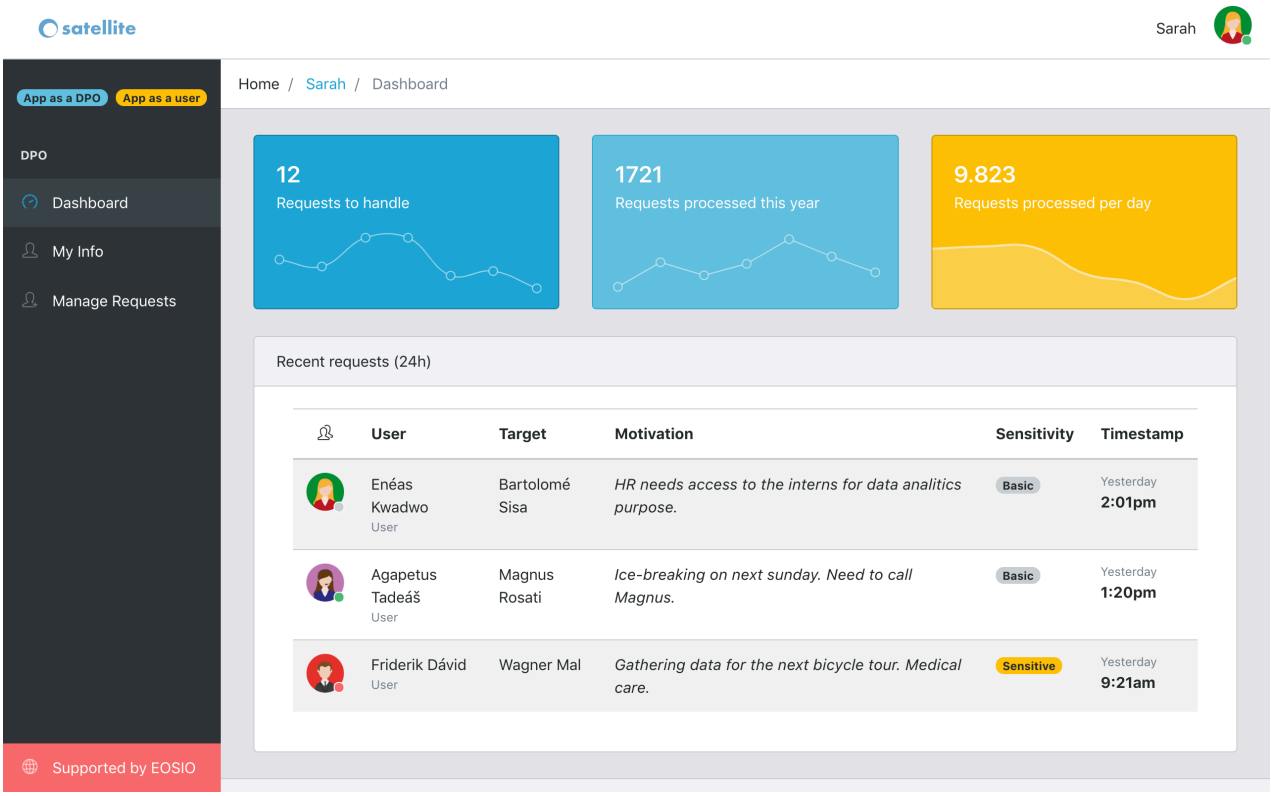
Satellite UI/UX

Prepared for: the jury
Prepared by: Antoine Laurens, Hugo Roussel, Vincent Ballet, Hugo Moreau, Paul Nicolet
23 September 2018

Satellite aims at providing an efficient tool to help companies in their chase to GDPR compliance. This new regulation requires corporations to be totally transparent on personal data management, with the right for each employee and customer to be forgotten. Satellite focuses on the internal side of a company and provides the data privacy management team with a solution to be liable to this kind of GDPR requirement, by using blockchain as an immutable and transparent witness of access rights. Using state of the art cryptography schemes, Satellite cannot leak data, guarantees a correct overview of what we call a chain of trust around your personal information, still maintaining the right to be forgotten.

LOOK & FEEL

The general look and feel of the app is oriented towards dashboards presented the different available informations to users. As a global idea, here is the main view of the Data Protection Officier:



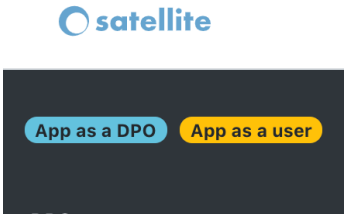
The design is based on CoreUI (https://github.com/coreui/coreui-free-bootstrap-admin-template), a CSS template built on top of Bootstrap 4. CoreUI proposes minimalists graphical elements in order to provide users with a great experience.

ROLES

There are two different roles on the platform:

- **Data Protection Officer** (DPO): this person is responsible for the personal data management in the entire company following the GDPR law. It is liable and trusted, and hold keys to access data of all the employees. The DPO also plays are interface between third parties and employees to access management.
- **Employee**: employees are owners of their own data and decide to modify, add or delete personal information. For some sensitive manipulation, the DPO must review the operation before being committed.

For the sake of the hackathon, it is possible to simulate both roles on the UI on the top left corner of the screen:



SENSITIVITY LEVELS

It is important to note that we make the distinction between two sensitivity levels for personal data: sensitive and non-sensitive (or basic) personal data. It essentially provides a way to decide if it is necessary for the DPO to have the agreement from the data owner before any third party new access. If the data is basic, then the DPO can decide on its own, keeping in mind of course that this is transparently logged in the blockchain.

DATA PROTECTION OFFICER

The main dashboard provides an overview of the activity of the personal data flow in the company, allowing to get quick insights on anomalies in the access requests across time, for example. The DPO can also have a look at its duty for the day with the descriptions of a few requests which need to be handled.
The screen on the right shows the request management view. From here, the DPO can decide which employee has the right to access to personal data of which target. Third party companies also interact with the DPO through this request mechanism allowing an equivalent transparency system. We can see that the DPO can either accept or rejet request. In case of a sensitive request, the feedback of the data owner will be required.

SATELLITE

satellite

Sarah

App as a DPO | App as a user

DPO

- Dashboard
- My Info
- Manage Requests

Home / Sarah / Dashboard

12
Requests to handle

1721
Requests processed this year

9.823
Requests processed per day

Recent requests (24h)

User	Target	Motivation	Sensitivity	Timestamp
Enéas Kwadwo User	Bartolomé Sisa	*HR needs access to the interns for data analitics purpose.*	Basic	Yesterday 2:01pm
Agapetus Tadeáš User	Magnus Rosati	*Ice-breaking on next sunday. Need to call Magnus.*	Basic	Yesterday 1:20pm
Friderik Dávid User	Wagner Mal	*Gathering data for the next bicycle tour. Medical care.*	Sensitive	Yesterday 9:21am

Supported by EOSIO

satellite

Sarah

App as a DPO | App as a user

DPO

- Dashboard
- My Info
- Manage Requests

Home / Sarah / Manage Requests

Pending requests

User	Target	Motivation	Sensitivity	Timestamp	Validation
Yiorgos Avraamu	Bartolomé	*HR needs access to the interns for data analitics*	Basic	Yesterday 2:01pm	✓ ✗
Quintin Ed			Sensitive	Yesterday 9:21am	✓ ✗
Enéas Kwadwo			Sensitive	21/09/2018 9:23pm	✓ ✗
Agapetus Tadeáš	Greta Diego	*Needs information to compute taxes.*	Sensitive	21/09/2018 2:48am	✓ ✗
Agapetus Tadeáš	Bali Mose	*Survey on gender and ages of all the employees.*	Basic	18/09/2018 4:11pm	✓ ✗
Agapetus Tadeáš	Gondo Lon	*Holiday checks, we need to know how many children the employees have.*	Sensitive	18/09/2018 10:34am	✓ ✗

Success ✓ ×

The authorization has successfully been granted.

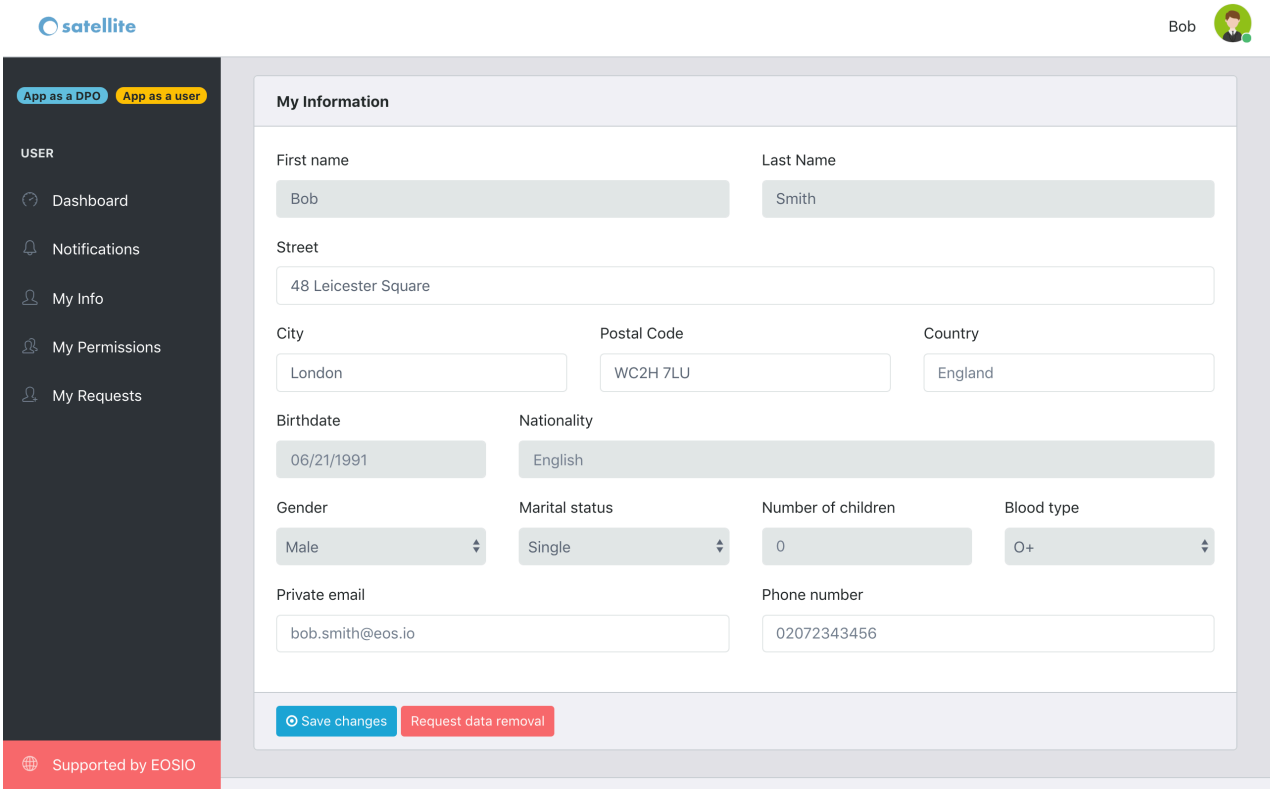
Close

Supported by EOSIO

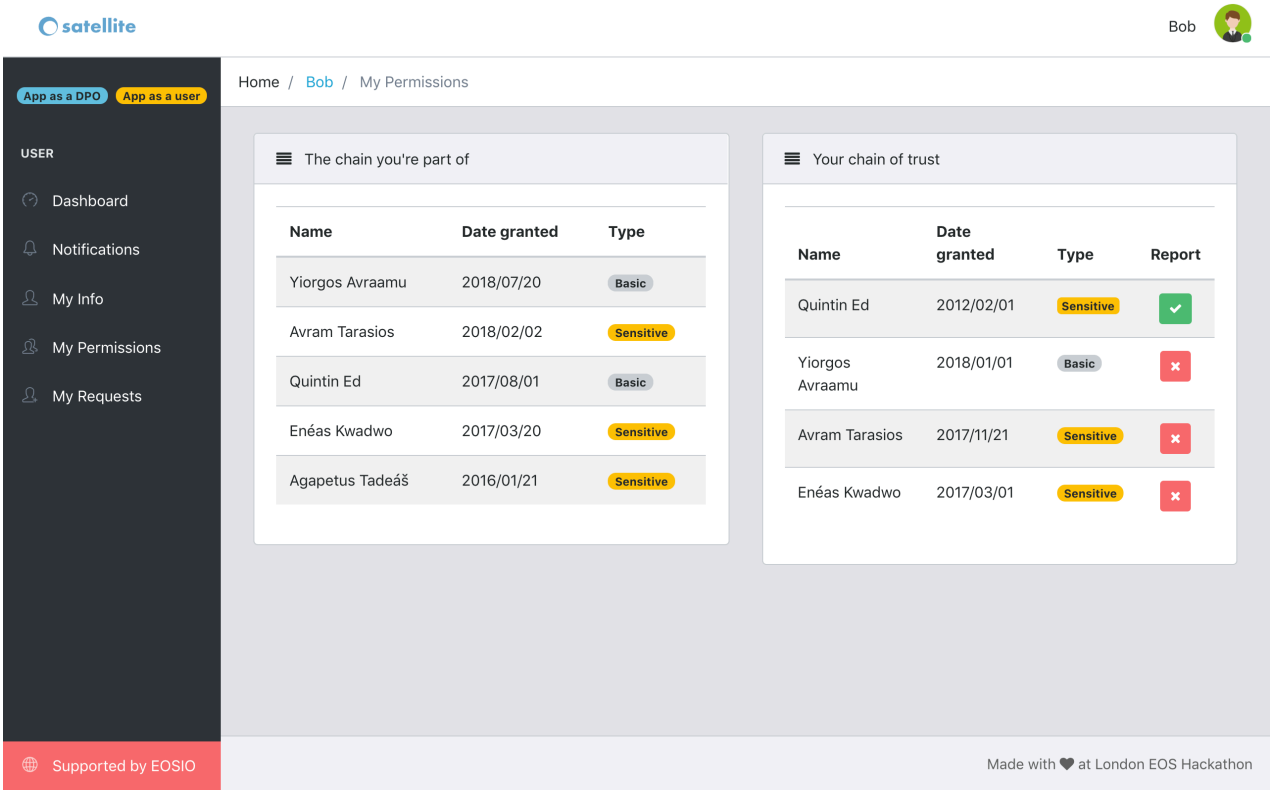
Made with ♥ at London EOS Hackathon

EMPLOYEE

The rights of the employees are to monitor, modify, add, or delete personal information. The left screen below shows the personal information page of Bob. The gray fields are the fields which are defined as being necessary for the company to operate smoothly, and cannot be modified without the DPO agreement. However, an employee can modify or even delete other information at any time at free will.



The second view represents the accesses. The left part shows the accesses you have asked in the past and have been granted to you. You are part of their chain of trust. The right part on the other hand is your very own chain of trust, with the rights to manage at any time third parties accesses. It is possible to see in this particular case that the first request needs to be approved because it treats sensitive data. The DPO accepted the request and is waiting for your approval.



Obviously, it is also possible for employees to generate requests to other employees to access their personal information. We can imagine an example where the accounting people need to access the current salary of all other employees.