User Guide

Data Owner

Introduction

Purpose
This guide aims to help users with a data "owner" role, i.e., users who consent to the processing of their personal data and acting as data subjects according to GDPR, on how to use the smashHit platform and gives knowledge about the different functionalities available.

Audience
This guide is meant for and solely for users of the smashHit platform with data owner role. Other roles can find their own user guides under smashhit.eu.

Scope
The contents of this guide are meant to be taken into consideration only when using the smashHit platform and will only cover functionalities meant to be used by the role stated above.

The smashHit team does not take responsibility for improper use of the application or the data provided when not following the instructions given in this guide.

Troubleshooting
For any questions or inquiries about the use of the smashHit platform web application or the contents of it or this guide, or if you find there is no content in this guide for some functionality, please forward it to: info@smashhit.eu

Contact
smashHit Project website: https://smashhit.eu

smashHit platform support: info@smashhit.eu

Contents

Guide

Basic knowledge

The objective of the smashHit framework is to assure trusted and secure sharing of data streams from both personal and industrial platforms, needed to build sectorial and cross-sectorial services, by establishing a framework to facilitate the processing of data subject consent and legal rules and effective contracting, as well as joint security and privacy preserving mechanisms. While these data streams offer new opportunities to build innovative services, they often require the management of a complex set of consent chains.

The main goal of smashHit is thus to overcome these obstacles by offering a set of methods and tools to facilitate the management of consents, supported by semantic models of consent and legal rules. The new tools include traceability of use of data, data fingerprinting and automatic contracting among the data subjects, data controllers and data processors.

Step by step

The main goal of smashHit for data owners is to provide a generic, transparent way to view and manage consent certificates and preferences. A standard step-by-step platform usage would look like this:

1- Data owner account creation: As the data owner grants their first consent to any organization that uses the smashHit framework for consent management, their data owner account will be automatically created by smashHit. To facilitate things, the organization is already collecting the necessary details for their account, so there is no need for the data owner to register manually in smashHit. Once the account is set up, the data owner will receive a welcome email with details on how to access smashHit.

2- Consent management: in the same way the registration is handled from an organization's application directly (and managed with the smashhit framework in the background), applications will present the data owner with a consent form (based on the consent templates previously defined for the application). Once the consent is created and communicated to smashHit, the data owner can log in to their profile to check the consent details and modify the selected options, which will be informed back to the applications involved.

3- Context and security preferences: data owners can also set their context and security preferences so that this will allow them to have a validity control of their consents by dates and hours or for vacation dates validity. In turn, they can also have the purpose and sectors at their whim in case these decide to be changed at some point in the contract.

4- Finally, users can of course manage their account through their profile settings in order to change their password or generally manage their account.

Consent management

Contrary to organizations, data owners are not expected to register on their own in smashHit, their registration is instead triggered (and handled) from the organization's applications using smashHit framework APIs. Figure 1 below summarizes how smashHit handles the registration of data owner users and their consent:
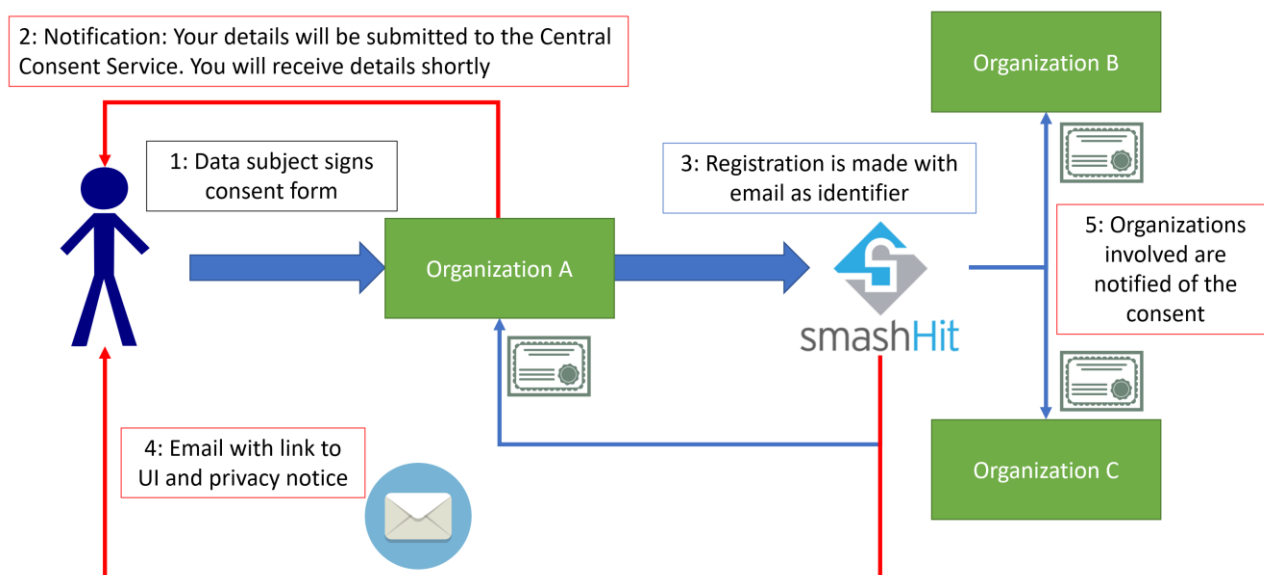

Figure 1: smashHit initial registration & consent management

1. Organization A, which uses smashHit for consent management, asks one of its users (data subject) for their consent
2. Organization A confirms the reception of the consent form to the data subject, and asks smashHit to process the consent request accordingly
3. smashHit automatically creates an account for the data subject using the email provided in step 1. The consent is validated, signed and stored in smashHit
4. The data subject receives a welcome email from smashHit, confirming their registration and providing instructions on how to access the smashHit UI at https://smashhit.ari-mobility.eu (Figure 2) to manage their consents.
5. The consent is notified to any organizations involved in the data processing, for example:
   a. Organization B might be a car company that needs to receive the consent to start providing data to Organization A
   b. Organization C could be tasked with performing a specific data processing on behalf of organization A

Figure 2: smashHit landing page

So, from the landing page, the data owner user would use their assigned credentials to sign in. smashHit manages its user accounts internally using the well-known FIWARE IdM (Identity Manager) Keyrock[1]. This enables smashHit to provide a robust single sign-on system that organizations can integrate in their applications too.

The first time accessing the web interface, the IdM will present a confirmation message (Figure 3) to authorize smashHit GUI to read its public profile information (the email address and the assigned role "data owner"), so that we can smashHit can properly present the interface and information according to your account and role.
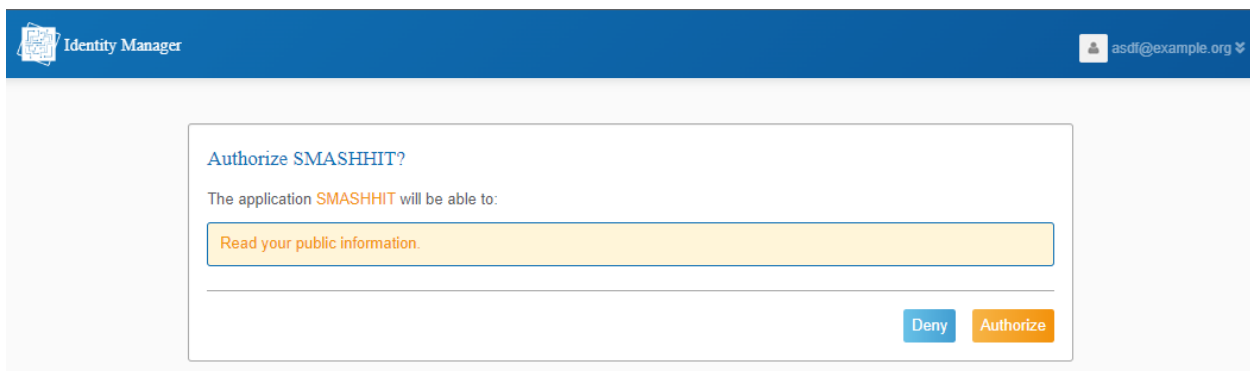
Figure 3: First sign in confirmation

Once in the platform, data owners can check the active consent certificate for each application they have interacted with in the context of smashHit, as seen in Figure 4.

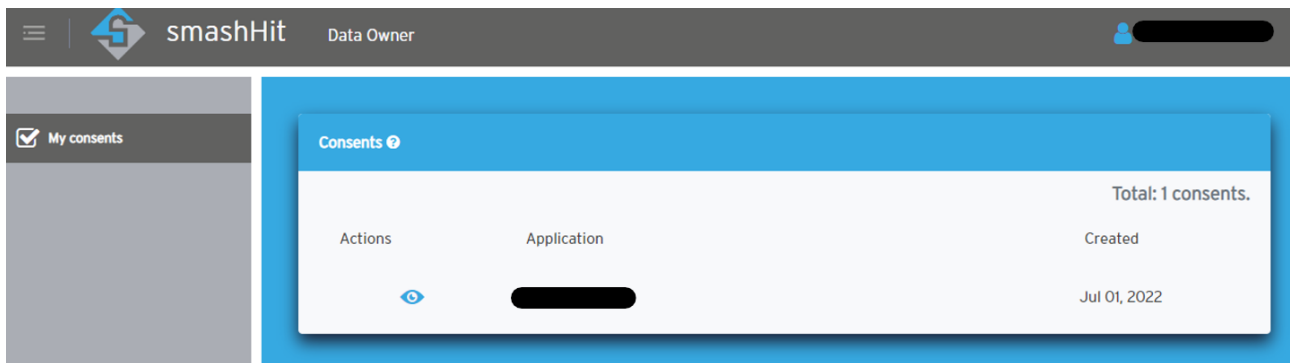[1] https://fiware-idm.readthedocs.io/en/latest/

Figure 4: Data owner certificate list

From here, data owners can check consent certificate details as well as modify their current granted consents (Figure 5, Figure 6, Figure 7) for which the platform will issue the necessary revoke/grant requests internally and notify the agents affected so they can take the necessary actions to enforce the new user decisions.
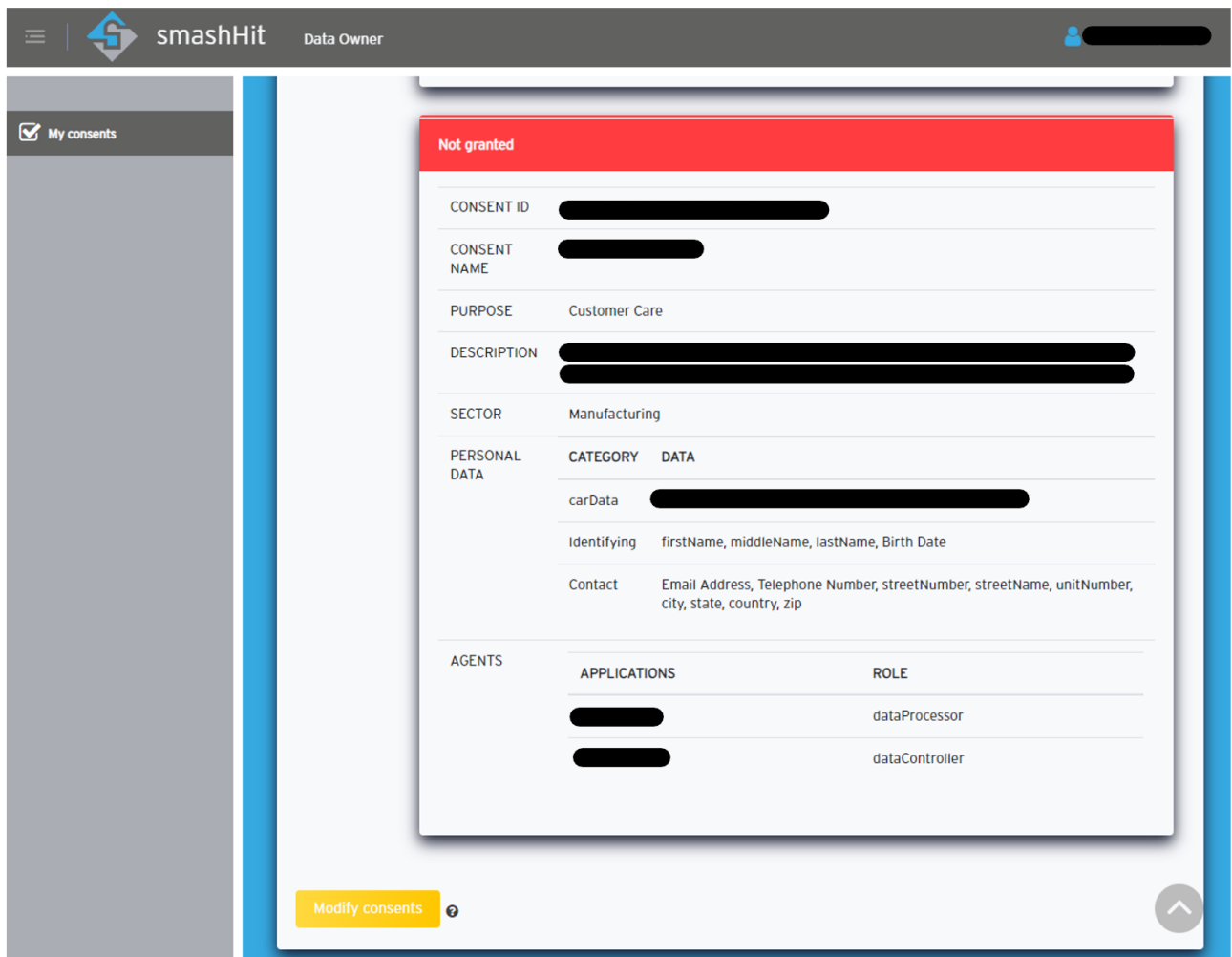

Figure 5: Consent modification (I)

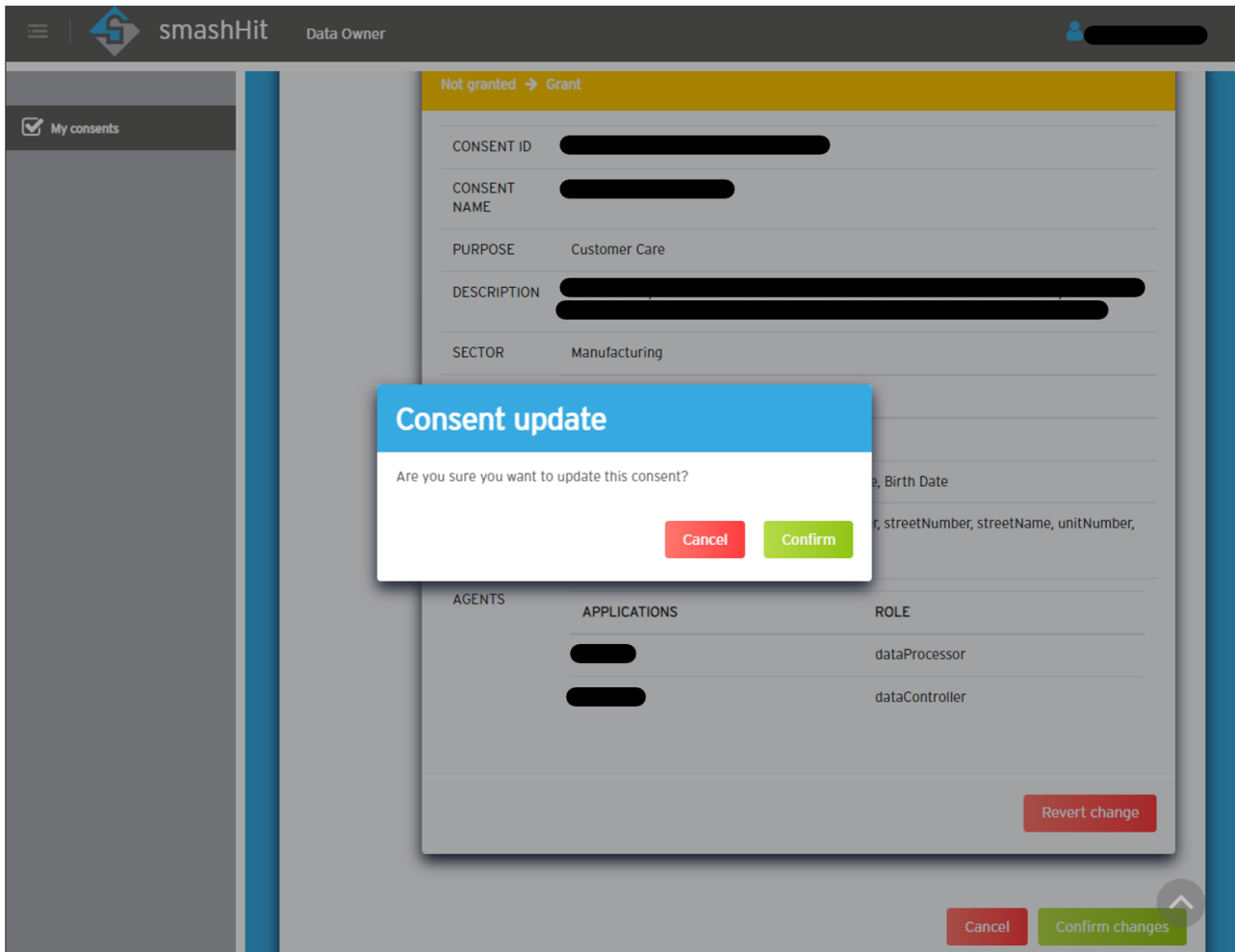Figure 6: Consent modification (II)

Figure 7: Consent modification (III)

Account management

By clicking its email address at the top-right corner (Figure 8), the user can access common profile and account settings configuration pages.
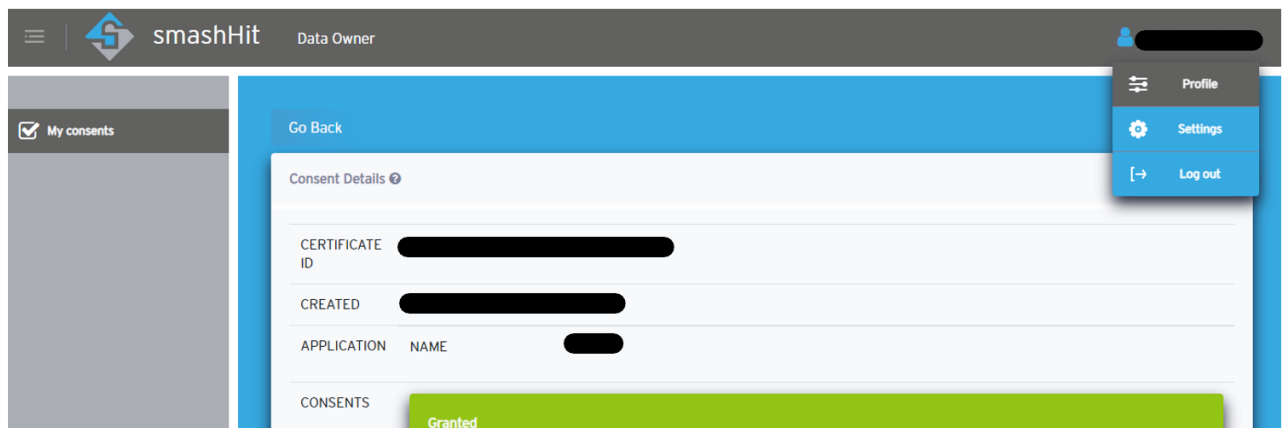

Figure 8: User profile & settings menu

From the "Profile" option, the user can check its account details (Figure 9) and manage them from the Identity Manager (Figure 10).
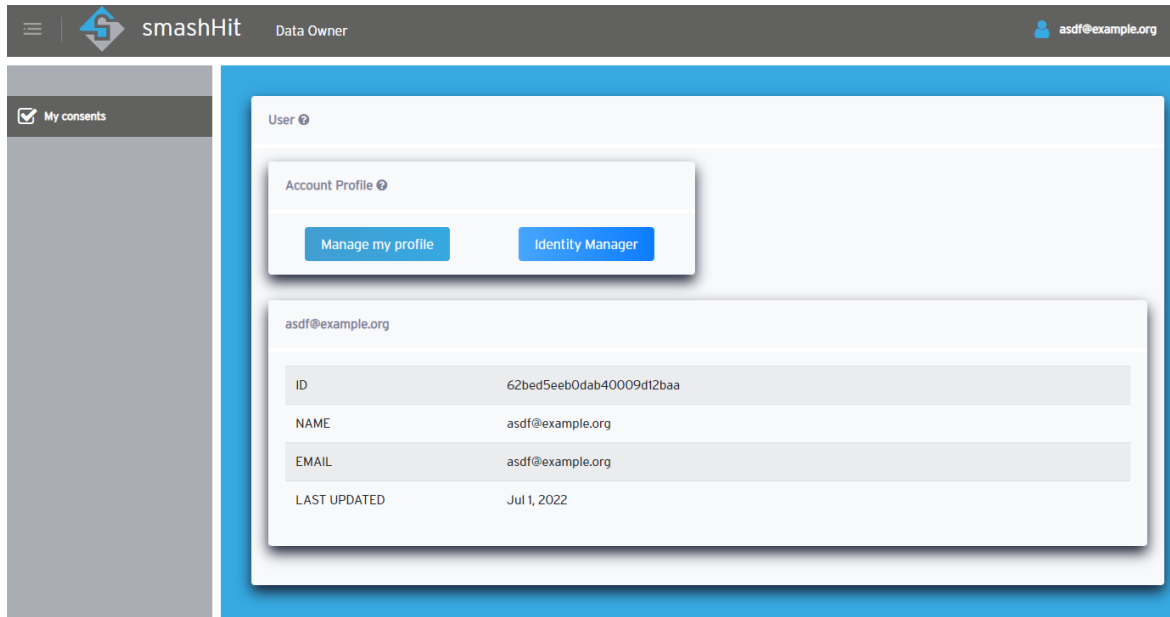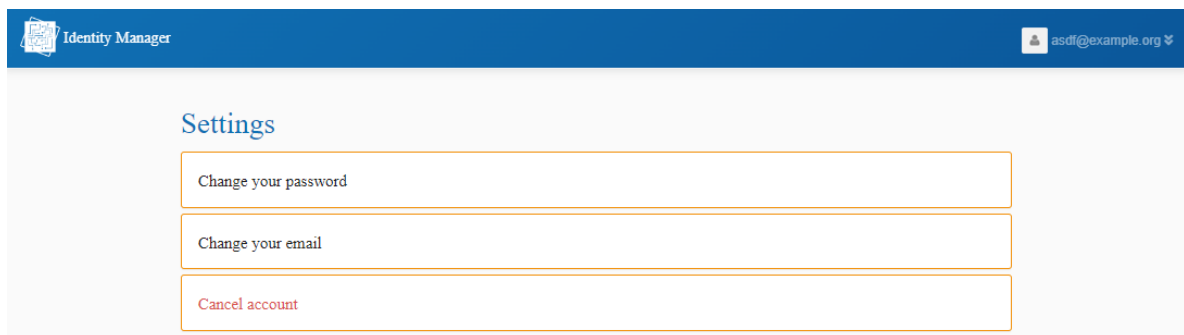
Figure 9: User profile

Figure 10: Account management through the IdM

The "Settings" option (Figure 11) allows the user to further configure their profile and review the privacy policy [2]. It is from here that data owners can configure their context and security preferences, as presented in the next section.
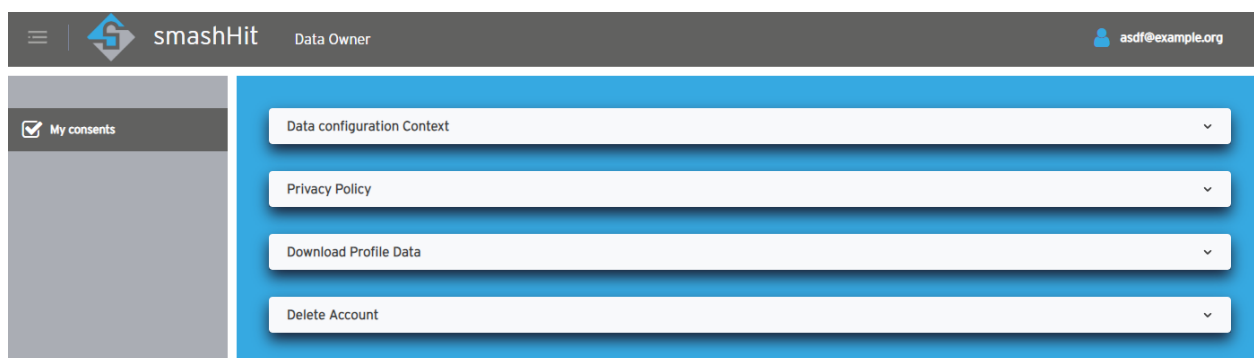

Figure 11: User settings

---

[2] For privacy policy information, please refer to smashHit's "Policy Guidelines"

Context and security preferences

From the Data configuration Context, the data owner will be presented with some options as seen in Figure 12. Here, the user can select their desired context preferences associated with the consents, such as purposes and sector.

After the new options are processed and stored by the smashHit system, any existing consents for the user will pass a compliance check to detect any conflicts with the new preferences. Any conflicts detected by the CSS will be reported via email to the data owner, so that they can manually review each of the offending consents and choose if they want to issue a revoke request.
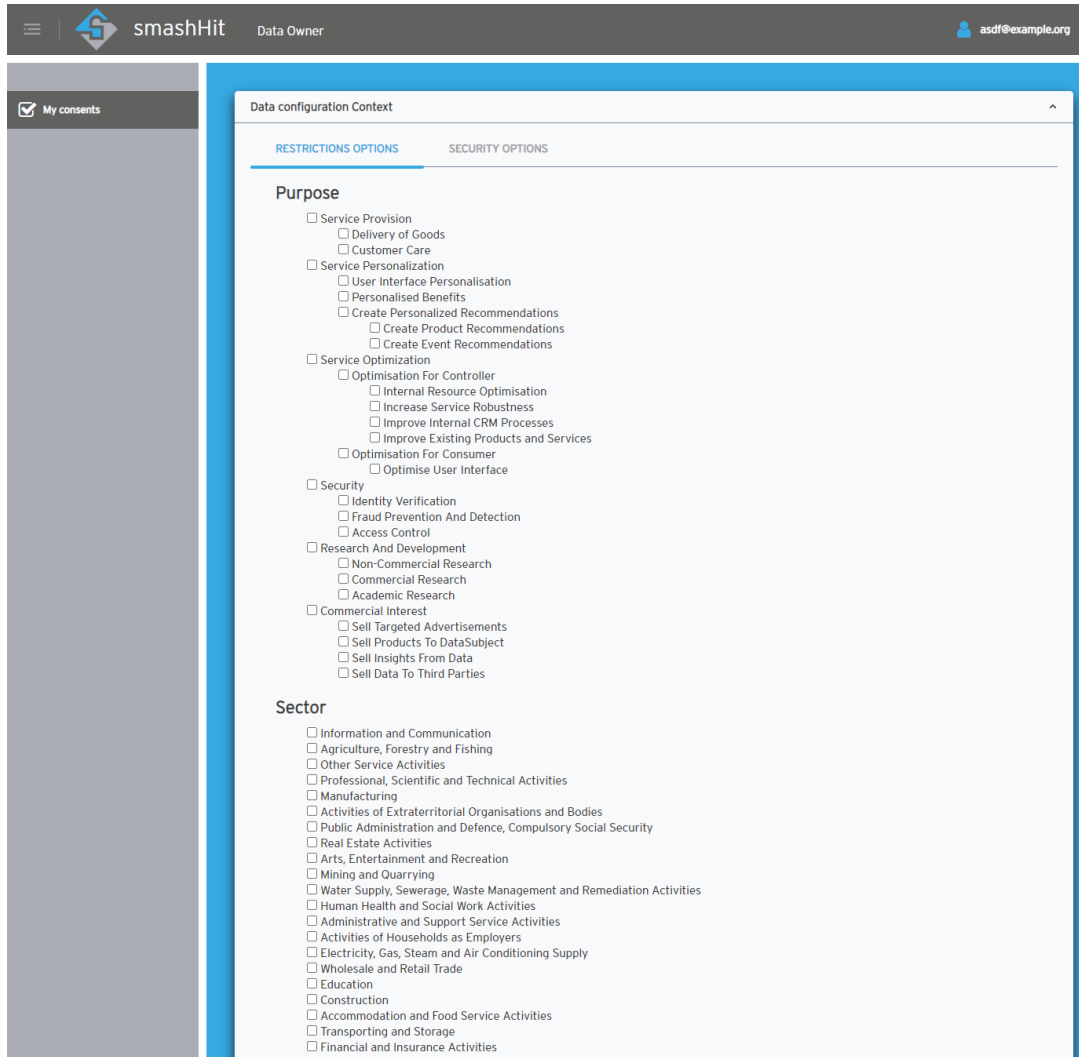

Figure 12: Context configuration options

The security options can be accessed from the same interface. In this case, the data owner will be presented with a similar form (Figure 13), where they can configure some policies mainly related to the date and time for which the consent is valid.

For example, a data owner might agree to share their car data only during business hours, for which they could set the holiday season and daily schedule so that it might be enforced.

Figure 13: Context security configuration options

F.A.Q.

smashHit platform

Q: What is the smashHit platform?

A: smashHit is a platform that provides a generic, transparent way to view and manage consent supported by disrupting technologies such as traceability of use of data, data fingerprinting and automatic contracting among the data owner, data provider, and service providers.

Q: How can I join smashHit?

A: In order to make sure the process is as straight-forward as possible for data owners, your registration in smashHit will be automatically handled by us when you sign your first consent with any of the approved smashHit partners.

Instructions to access smashHit will be sent to the email address you've indicated to the organization requesting consent.

Q: What personal data does smashHit require?

A: smashHit will only use the email address provided by the organization to automatically manage your account. Even if a consent exists for sharing further personal data with any smashHit partner, such data won't ever be accessible to smashHit.

smashHit is an integral solution for consent management, but the personal data sharing flows between organizations is out of the scope of smashHit itself. Your personal data will always flow directly from the data "provider" (for example a car manufacturer) to the data "processor" (such as an insurance company).

smashHit is therefore not supposed to act as a man-in-the-middle in this data flow, but assist in managing and notifying the different actors about the consent: which personal data is to be processed and, the purpose of the processing, type of processing, and the role according to the GDPR (data controller/processor) of the different organizations involved.

Glossary

ACT: Automatic Contracting Tool

Agent: Entity that bears some form of responsibility in the context of a consent

Administrator: smashHit platform system administrator

Consent: As per Article 4(11) of the GDPR, 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her

Consent template: A template defining the details of a data processing by an Agent (smashHit organization user), such as the purpose of the processing or the personal data to be processed

CSS: Context sensitivity solution

Data owner: smashHit user role which acts as the data subject according to GDPR

Data subject: Legal term in the GDPR used in a context where personal data is processed determining the person to whom an information is or can be related. The data subject is a natural person who can be identified, directly or indirectly, by a factor specific to her or his physical, physiological, genetic, mental, economic, cultural or social identity.

DUT: Data Use Traceability

GDPR: Abbreviation for 'General Data Protection Regulation', a legal norm on EU level adopted in 2016, which is directly applicable within its scope and lays down rules for the processing of personal data so as to protect natural persons' fundamental rights and freedoms, in particular their right to the protection of personal data

IdM: Identity Manager

Personal data: Any information which are related to an identified or identifiable natural person (Art. 4 (1) GDPR), e.g. a name or a home address

Purpose: The purpose of Data Handling/Processing

Figures

> **Our vision** - Solving Consumer Consent & Data Security for Connected Car and Smart City

> **Further information**

This document is part of the smashHit Methodology. The complete set of documents, including other user/developer guides as well as white papers created within this scope can be found on our website:

https://smashhit.eu/publications

> **Our consortium**