socital
Personalised E-commerce.

Personal Data
and Processing Guide

by Socital, Last update: 1st of November 2018

Table of Contents

Summary

What does Socital do?

Socital is a service provider that helps e-commerce businesses increase their sales through personalization. Socital provides tools to collect, store, process and segment data of the client's visitors, subscribers and/or customers - collectively referred to as the End Users, and tools that produce personalized recommendations based on that data.

Socital is a Data Processor

The e-commerce business (Socital's client) is the data controller of its visitors', subscribers' and customers' personal data. Socital is an appointed data processor from its client and always acts on behalf of its client that uses Socital's services. The client should inform its users about appointing Socital as a data processor.

What Socital does with End Users' data

Socital extracts - ***with End User consent*** - stores and processes that data, to create a profile for the client's visitors, subscribers and/or customers. This profile may include Social, Identity, Interest, Browsing Behavior and Order data. It then produces personalized product recommendations and makes all that available to the client for export to other platforms that the client uses, such as email marketing platforms, CRMs and more.

What Socital doesn't do with End Users' data

- *Socital does not scrape the web or buy personal data from any third parties. All personal data that Socital handles on behalf of the client are either extracted with consent or given to Socital from its client with the purpose of processing.*
- *Socital does not share that data with anyone else other than the client and third-party sub-processors that Socital uses.*
- *Data are never shared between Socital's clients. Socital does not combine the data from different clients in the same End User profile, even if they may concern the same individual. Personal data are always stored and processed separately for each client, and no identity matching between different clients' End Users ever takes place.*
- *Socital does not keep personal data obtained on behalf of the client after the contract with the client ends.*

Definitions

Client: The company that uses Socital's services to collect, store, process and segment data of its visitors, subscribers and customers with the purpose of increasing its sales with personalization.

End User: the visitor, subscriber and/or customer of the Client. Socital extracts, stores and processes the personal data of the End Users on behalf of its Client.

Disclaimer

This material is intended for general information purposes only and does not constitute legal advice. For legal issues that arise, the reader should consult legal counsel.

Who are the data subjects

The personal data in question, pertain to ***the site visitors, customers and/or subscribers of Socital's client.***

Socital's client is the data controller of its visitors', subscribers' and customers' personal data, and therefore the data subjects agree to the Terms of Service and Privacy Policy of the client. Socital is an appointed data processor from its client and always acts on behalf of its client.

The personal data Socital stores

Socital extracts, stores and processes personal data of client's visitors, subscribers and/or customers on behalf of its client, collectively referred to as the "End Users".

The End Users' personal data that Socital handles on behalf of its client, are grouped in the following categories:

1. ***Social, Identity and Interest Data***
2. ***Browsing Data from client's site***
3. ***Commerce Data***

A. Social, Identity and Interest data

How are Social data obtained?

Social data are always obtained with the consent of the End User. The data are extracted from the End User's Social Network profile through the Social Login mechanism that is provided by the Social Networks. The data are then stored, and/or processed further and made available to the client for export.

Socital may also store free text data that End Users submit in Socital Plugins at the client's website, as well as other estimated Identity and Interest data that are produced from the processing that Socital does on extracted End User data, on behalf of its client. Those estimations may include an ***estimated Gender, Age Range, estimated Interests, Brand affinities and estimated Locations of Interest.***

The Social data that Socital extracts from Social Networks and stores on behalf of its client, may include the following, depending on what information the End User will choose to share and with which Social Network profile the End User will choose to login with.

Data that might be extracted from Social Networks

Facebook

First name
Last name
Email address
Profile picture
Gender
Age Range
Birthday
Location
Hometown
Timezone
Language in which the End User uses Facebook
Languages spoken
Education history
Work history
Facebook friends (count and friends using the app)
List of the liked Facebook fan pages
About (Bio)
Facebook Profile URL

Google

First name, last name and formatted name
Email address
Profile picture
Gender
Age Range
Birthday
Location
Language in which the End User uses Google
Places lived and current location of residence
Tagline
About me (Bio)
Skills
Organizations associated with and metadata such as title, location and more
Google Profile URL

LinkedIn

First name, last name and formatted name
Email address
Profile picture
Industry the End User belongs to
Headline and summary
Job positions and their metadata such as title, start and end date, location and more
Location
Language in which the End User uses Twitter
Languages spoken
Education history
Work history
Number of connections on LinkedIn.
Specialties
LinkedIn Profile URL

Twitter

Name
Profile picture
Location
Timezone
Language in which the End User uses Twitter
Languages spoken
Description (bio)
Number of followers and accounts followed by the End User on Twitter
Twitter Profile URL
Twitter statuses and their metadata

B. Browsing Data from client's site

Socital can track the client's visitors browsing behavior on the client's website. The browsing behavior is used to determine products, product categories and/or brands that the visitor is interested in, with the purpose of producing personalized product recommendations and assisting the client to perform relevant targeting campaigns.

Socital ***does not*** synthesize the browsing behavior of the same individual on websites of different clients. Socital tracks, stores and processes the browsing behavior of website visitors for each client separately.

How are Browsing data obtained?

Socital tracks the pages that an anonymous visitor views on the client's website through the Socital script that the client adds in the <head> tag of their website.

The collected browsing data are associated to a specific End User (visitor) profile, only if the End User subscribes to a Socital Plugin. As described in the Consent section, the client can utilize the available Generic consent checkbox on Socital Plugins and its Terms & Conditions to outline the necessary terms for associating browsing data with the End User's profile.

The Browsing Data that are stored and may be associated with a specific End User profile, include:

- *Referring domain from which the visitor landed on client's website*
- *URLs of pages visited on the client's website*
- *Interaction with Socital Plugins, such as viewed the Plugin, opted-in, clicked on product recommendations.*
- *Device type and device model.*
- *IP address*

C. Commerce Data

Socital gives the option to its clients to import their commerce data into Socital. The purchase information can then be used in combination with the Social, Identity and Browsing Behavior data to create Segments and to produce personalized recommendations also based on purchase history and products bought.

The Commerce data that may be imported into Socital and used for Segmentation and Recommendations are:

- *Email address (with which the order was placed).*
- *Address.*
- *Products bought and their value.*
- *Timestamp of Order.*

How and when Socital got the data

All personal data that Socital handles on behalf of its client are either extracted with consent or given to Socital from its client with the purpose of processing. Socital does not scrape the web or buy data from any third parties.

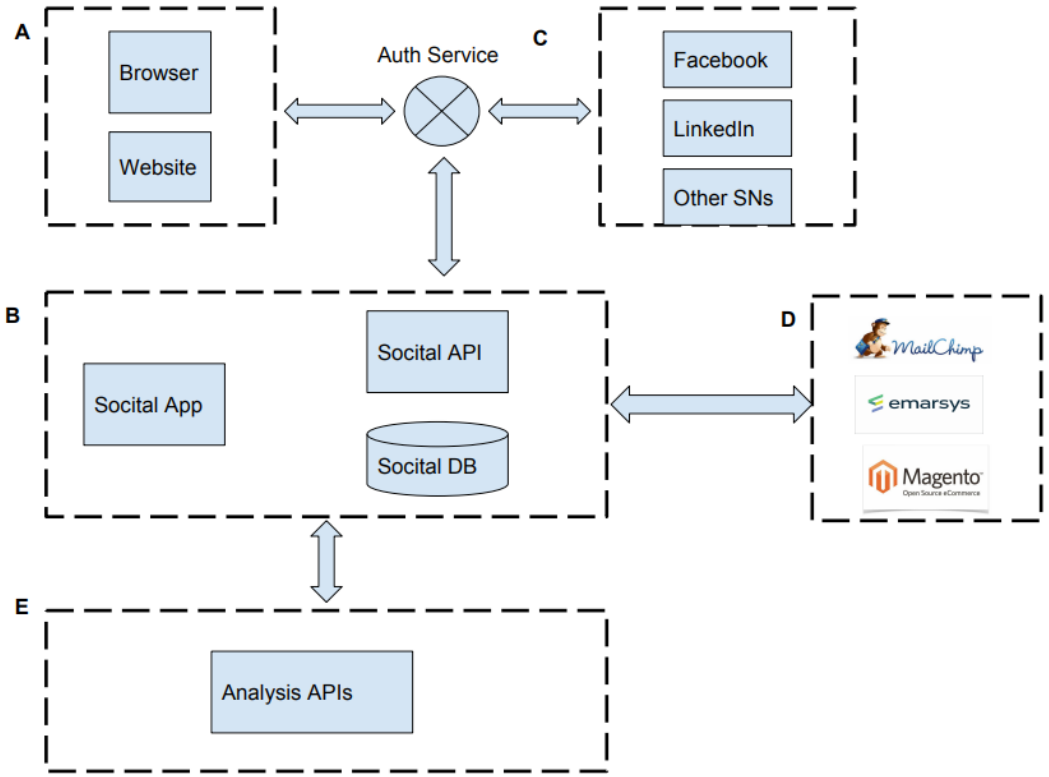
The client - being the data controller, is responsible to ensure that all necessary consents have been obtained from the End Users regarding the processing of their data, before importing any personal data into Socital.

Socital also gives the tools to its clients to request explicit consent on Socital Plugins.

There are various ways with which personal data are imported into Socital and all require client's action to be performed. Specifically:

- *Social data: Social data are always obtained with the consent of the End User. The Client can add a Socital Plugin to their website (a popup or a lead generation form). End Users can opt into a campaign through those Socital Plugins by subscribing with their email address or by connecting a Social Network Profile. Socital then extracts the social data - on behalf of its client - from the End User's Social Network profile. The mechanism that is used, is the Social Login mechanism and the Social Network API as provided by the Social Network.*
- *Browsing Behavior data: Socital's clients can add the Socital tracking script on their website, and configure it to track specific events, such as page views, add to cart events and more. Once an End User opts-into a Socital Plugin the tracked Browsing Behavior is then associated with the End User's profile and used for personalized recommendations.*
- *Existing Email databases: Socital's client can use the User Interface at my.socital.com to import a file (CSV) with their existing email database to analyze for Gender, Age and more.*
- *Commerce data: the client can import Commerce data through the Socital Public API or by using the integrations that Socital has with commerce platforms - such as Magento. To use the integrations, the client needs to add their unique and secret API credentials provided by the commerce platform and trigger the import and sync of the data.*

Data Flow Map



- *End Users access the client's website from their browser (Component A).*
- *Socital's "Auth Service" handles communication between Components A, B, C and extracts the Social Network data based on the End Users permission.*
- *Authorization process is carried out through the well-established OAuth2 protocol over secure HTTPs connections.*
- *Personal data is stored in "Socital Database" of Component B.*
- *Component B infrastructure is deployed on Microsoft Azure cloud services.*
- *Data may be transferred to external APIs for processing (Component E).*
- *Data may be exported by the Client to third-party services that the Client uses (Component D).*

Consent on Socital Plugins

Socital provides Plugins to create and launch onsite campaigns on the client's website. Such campaigns include newsletter subscription forms, discount coupons, contests, contact forms and more.

Socital gives the option to its client to add a consent checkbox on all onsite campaigns. The client should enable the consent checkbox and add the appropriate consent text to ensure that all End Users that participate in the campaigns give their explicit consent to collect, store and process their data and any other terms that are necessary for the End User to use the client's services.

From 25th of May, Socital will give the option to its Clients to differentiate between two types of consent in Socital Plugins. A "Generic" consent where the Client can include any Terms they deem necessary and appropriate and a "Marketing" consent regarding receiving promotional communication.

What Socital does with the data

Socital extracts - with consent, stores and processes the data, to create a profile for the client's visitors, subscribers and/or customers that may include Social, Identity, Interest, Browsing Behavior and Order data.
It then produces personalized product recommendations based on the aforementioned data and makes all that available to the client for export to other platforms that the client uses, such as email marketing platforms, CRMs and more.

More specifically the ***End User's data may be processed in the following ways:***

- *Analyze the profile picture to estimate Gender and/or Age Range.*
- *Analyze the first and last name to estimate Gender and normalize and/or translate the first and last name.*
- *Analyze the email address to estimate Gender, normalize and/or translate the first and last name, and/or the organization and country associated with.*
- *Analyze Facebook likes to estimate Brand Affinities, Interests, Locations of Interest and Spending Capacity.*
- *Analyze the languages information from Social Network profile or browser to estimate spoken languages and whether the End User is an English Speaker or not.*
- *Estimate Location - country and/or city - from the IP address.*
- *Generate personalized recommendations for each End User by combining and analyzing the Social, Identity, Browsing Behavior and purchase history.*

Where that data reside

All of Socital's assets where also the End Users' personal data are stored, are hosted on ***Microsoft Azure cloud platform***. Socital operates solely on Virtual Machines. That is, Socital uses only "boxes" and handles deployment and server management (no 3rd parties involved).

The data is hosted on a set of ***dedicated*** Virtual Machines hosted on Azure and managed by mLab on the same Microsoft Azure region.

Physically, the Microsoft Azure region selected is ***"North Europe"*** (UK - Ireland).

Encrypted backups of the data are hosted on bare-metal physical servers provided by Hetzner (physically located in Germany).

Who can access the data and what can they do with it once they do

The Client

- ***From the Socital app at my.socital.com:*** *Socital's client is the data controller and can access the data through their dedicated account at the Socital App found in my.socital.com. To access their account, the client's operator needs to enter their username and secret password. Once the account is accessed, the client's operator can view the End User's profiles and data. He can also export the data to a CSV or to other third party platforms that the client uses and has connected with their Socital account, such as their email marketing service, CRM etc.*
- ***Socital Public API:*** *The client can also access and export the personal data through the Socital Public API using their unique and secret credentials.*

Socital Senior and/or Lead Software Engineer

Socital' senior or lead software Engineer may access the Servers and/or Databases where the personal data are stored to perform deployments, debugging and/or restore backups.

Engineers may also access the data to perform authorized extraction, editing *and/or deletion of specific End User data when specifically requested by the client and in accordance to the General Data Protection Regulation.*

The engineers' access is secured in the following ways:

- *Connection to application servers uses standard SSH protocol.*
- *Database connections use TLS/SSL connections*
- *Access logs are being kept.*
- *Socital follows a strict policy on producing and retracting access credentials for engineers during onboarding and offboarding.*

How long Socital stores the data

Socital stores the personal data for as long as it's contracted by the client. The personal data collected and/or imported are necessary to be retained for that period, in order to regularly generate personalized recommendations and insights that are used by the client in its frequent targeting campaigns. When the contract with the client ends, the personal data that were collected, imported and stored on behalf of the client are deleted.

Security Measures

All of Socital's assets where the End Users' personal data are stored, are hosted on Microsoft Azure cloud platform. Socital operates solely on Virtual Machines. That is, Socital uses only "boxes" and handles deployment and server management (no 3rd parties involved).

Measures taken for data security:

- *Communication with external systems (e.g browsers) is done over secure HTTPS connections (HTTP request are redirected to HTTPS as well).*
- *Connection to application servers uses standard SSH protocol.*
- *Database connections use TLS/SSL connections.*
- *Backups are encrypted.*

Access Control

- *Requests to new access permissions are subject to approval by a Senior Engineer or the CTO.*
- *Individual accounts are used for all activities performed by humans (i.e., not cronjobs, automated scripts, etc.).*
- *Key systems enforce regular password and/or access keys changes*
- *There is a process that ensures the removal of unneeded permissions from users who left the company or changed roles*

Data Location

- *All Socital's customer data are stored within the EU (Microsoft Azure data centers)*

Documentation

- *Detailed data flow diagrams and data inventory (data allocation) documents are readily available and can be provided (to the client) upon request.*

Infrastructure

- *Development, testing (staging) and production environments are strictly segregated both from a system and data perspective (i.e., not using production data is used in development and testing systems)*
- *Physical development terminals / workstations locked automatically after a predefined period of inactivity*

Logs

- *Logs are regularly monitored or reviewed from a security perspective*
- *Logs are protected against accidental or intentional modification*
- *Encryption in transit is applied for all sensitive communications*
- *All of Socital's data centers resources are dedicated and not shared by other cloud platform users.*

Data Backups

- *Data backups are taken regularly*
- *No backups are held off-site*
- *All backups are encrypted*

Networks

- *Firewall rules protect all Socital's cloud platform and cover all traffic*
- *Firewall rules are reviewed regularly*
- *Firewall rules changes are approved by the CTO*

Organization

- *Socital has assigned a dedicated DPO able to assist in any matters related to security*
- *Employees are regularly trained in security best practices*
- *All employees sign a confidentiality or non disclosure agreement*
- *There is a process for terminating user access privileges when they are no longer needed, i.e. when someone changes for and/or leaves the company.*
- *In case of data breach there is an incident response procedure in place.*

How Socital facilitates requests to delete, edit and cease processing of personal data

End Users have certain rights regarding their personal data. End Users direct those requests to the client who is the data controller to whom they have initially given the permission to collect and process their personal data. End Users may ask to get a copy of their personal data, have them rectified, have them deleted or they may opt-out from processing.

If the Client receives any such request, the client should submit a formal and written request to Socital at ***dpo@socital.com*** mentioning the email address of the End User and the details of the request. The client is responsible for verifying the identity of the individual before submitting the request to Socital.

Who Socital shares the data with

Socital does not share that data with anyone else other than the client and third-party sub-processors and service providers that Socital uses. Data are never shared between Socital's clients. Socital does not synthesize the data from different clients, even if they may concern the same individual. Personal data are always stored and processed separately for each client, and no identity matching between different clients' End Users ever takes place.

Sub-processors that Socital uses:

- ***Microsoft Face API*** *is part of Microsoft's Cognitive Services APIs. Face API is used to detect, identify and analyze human faces in photos.*
- *IMI Ideas and Development Athens - Socital's Greek sub-contractor.*

Countries Socital transfers data to

The data are stored within the EEA region, at a Microsoft Azure data center (*"North Europe"*: UK - Ireland) and at Hetzner in servers physically located in **Germany.**
IMI Ideas and Development Athens is located in **Greece** and for the Microsoft Face API Socital makes use of the North Europe service endpoint.

How data gets deleted

Upon request, given a SUID / email, a separate process removes the necessary records from the primary database (MongoDB), events database (Postgres) indexed copies of the data (ElasticSearch) and associated backups.