Statement on Data Processing Structure in regard to accessWidget SaaS solution, issued by accessiBe Ltd. to AccessiWay s.r.l.

Premises

1. Our business is not based on the commercialisation of data but on provision of digital accessibility solutions. The purpose of our company's products is to make the web accessible and we do not attempt to generate revenues from data commercialisation.
2. Our "accessWidget" tool sends the following data to our servers:
   - image URLs;
   - link URLs;
   - HTML structure;
   - CSS attributes;
   - clicks;
   - interactions;
   - pages viewed;
   - number of pages;
   - number and date of scans.

   This information is associated to the domain on which the widget is installed and not an user; moreover, it does not include actual content/text from the web page or form or field information. In addition, the foregoing information does not include any Personal Information of any person viewing a website on which accessWidget is installed (a "User") and cannot be associated with any User.
3. Other than as stated herein, we do not process any personal data of Users.

Overview

This paper aims to describe which data is transferred from the User session to accessiBe's servers through accessWidget. accessWidget's script that is installed on a website requests resources from the accessWidget servers (JavaScript code, metadata resources). These requests originate from the User's browser session and land in accessWidget's proxy server inside the European Union. The requests are described below and for each request some data of the User's browser session is transferred to the servers as described below.

The data that are transferred are the default headers sent by the User's browser whenever a User hits any internet page. So, these data are not required to let accessWidget works properly, but are only mandatory data that a client/server request requires.
There is no technical solution to avoid sending this data, therefore we implemented the proxy server solution to ensure that this data cannot be linked to any specific User and are completely anonymized within the European Union.
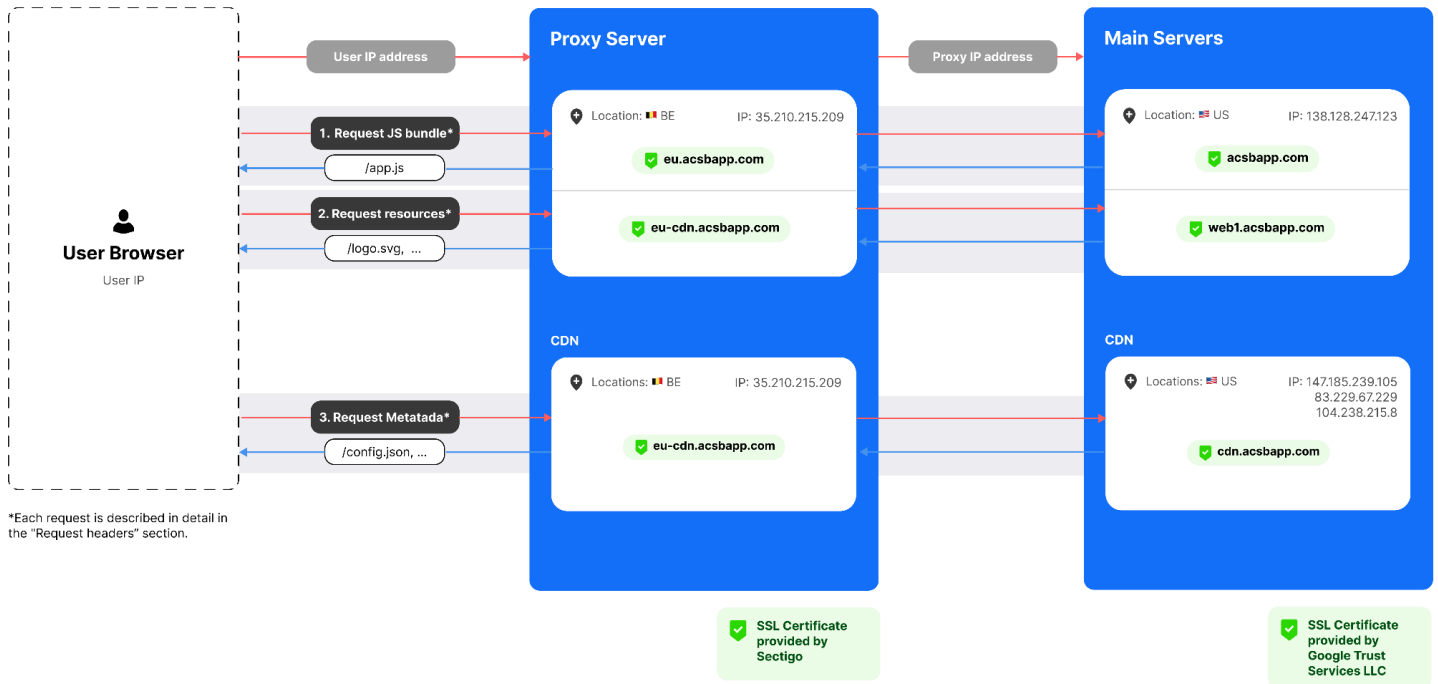
European Proxy

All the requests coming from Europe are redirected to the European Proxy Server located in Brussels and from here the requests are forwarded to the main servers located in the United States. During this forwarding only the proxy's informations goes to the main servers: through this feature we ensure that user data (such as IP address) never goes outside the European Union.
To summarize: all user data from the European territory will never go outside, and the only data that reaches the servers in the U.S. is the proxy server data.

Data transferred

All the data transferred from the User with those requests are not saved on accessiBe's server and are only used to send back the necessary code to the User's browser. We do not save any logs related to this data.

Request headers

With each request the IP address of the User is used in the communication. Generally, User's use dynamic IPs that change constantly.

1. Request JS Bundle

Key	Value
:method	GET
:authority	eu.acsbapp.com
:scheme	https
:path	/apps/app/dist/js/app.js
:sec-ch-ua	**Informations about the browser used**
sec-ch-ua-mobile	**Client is mobile**
user-agent:	**Informations about the computer used (model, version)**
sec-ch-ua-platform	**Operating System**
accept-language	**Language of client**
accept:	*/*
sec-fetch-site:	cross-site
sec-fetch-mode	: no-cors
referer:	website url

2. Request Resource

Key	Value
:method	GET
:authority	eu-cdn.acsbapp.com

:scheme	https
:path	/apps/app/dist/media/logomono.svg
:sec-ch-ua	**Informations about the browser used**
sec-ch-ua-mobile	**Client is mobile**
user-agent:	**Informations about the computer used (model, version)**
sec-ch-ua-platform	**Operating System**
accept-language	**Language of client**
accept:	image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0
sec-fetch-site:	cross-site
sec-fetch-mode	: no-cors
referer:	website url

3. Request JS Bundle

Key	Value
:method	GET
:authority	eu-cdn.acsbapp.com
:scheme	https
:path	/cache/app/website/config.json
:sec-ch-ua	**Informations about the browser used**
sec-ch-ua-mobile	**Client is mobile**
user-agent:	**Informations about the computer used (model, version)**
sec-ch-ua-platform	**Operating System**
accept-language	**Language of client**

accept:	*/*
sec-fetch-site:	cross-site
sec-fetch-mode	: no-cors
referer:	website url

Database Structure

To provide further confirmation that we do not store any data that is personal or linkable to specific Users, below is an explanation of how the database is structured.
We only save data related to the website domain on which accessWidget is run. Such information includes the number of pages on the website, number of scans, date of scans, date of data refresh (rescanning, reanalyzing, reprocessing), image URLs, links, HTML structures, CSS selectors, etc. None of these items are related to any User.

Security measures adopted

The following is a quick overview of the security measures taken on the data:
- storage: we do not store any data, so there is no need to encrypt them;
- transit: during the transit (HTTP requests) every data is encrypted. For this encryption we have SSL certificates provided by Sectigo (for communication with the proxy server) and Google Trust Services LLC (for communication between the proxy server and the main servers). The supported protocols are:
  - TLSv1.0;
  - TLSv1.1;
  - TLSv1.2;
  - TLSv1.3.

Company: AccessiWay S.r.l.

Address: Via Pietro Micca n. 20, Torino - 10122 (TO), Italia

By: Edoardo Arnello

Role: CEO