How we handle data at ClickPatrol.com

When a user clicks on an ad in Google Ads / Facebook / Bing, ClickPatrol.com is informed via a beacon directly from the Ad network (Google Ads / Facebook / Bing). The ad network then shares some information about the click and user with us.

How we process the information received

- **Step 1:**
  ClickPatrol.com hashes the data with an unique key IP address and device fingerprint data received are immediately hashed with a unique key and stored with campaign data.

- **Step 2:**
  We check the hashed data against our own database to find out if there is a match and we know the user.We then run the data received from our database through our algorithm to obtain more information and qualify the click. Our algorithm gives us 2 results a fraud number (the higher the number the more likely its fraud), and fraud reasons. Fraud reasons are reasons why our algorithm thinks the user is a fraud.
  This data is also stored.

- **Step 3**
  We also send the hashed header and IP to our data service providers who are (GDPR and CCPA proof). If this hashed IP exists in their database they share with us the external enriched data regarding this hashed header or IP.

- **Step 4**
  We run this new data true our algorithm again to get a response with 2 results a number and reasons.

- **Step 5**

  We combine these 2 results from and conduct a final check before we confirm it's an unwanted click or not.

Who has access to the data:

- Our Founder
- Our Lead developer
- Our Lead Data analyst

These individuals have signed a contract on data protection and data privacy according to dutch law.

Our system does not allow anyone make copies or export data.

Other important notes;

- We conduct all tests on sample data in an OTAP environment

How does this affect you (our users)?

When you log into your ClickPatrol.com dashboard you'll be able to see some collected data and some data related to the ip.

Since we don't store privacy related date all reports exported only contain non-privacy related data.

List of data points we use to detect fraud (when available):

From the Ad network:

- AdPosition
- Location of Interest
- Campaign ID
- Adgroup ID
- Keyword
- Google Network
- Device

- Placement
- Google ClickID
- Bing ClickID
- Facebook ClickID
- Ad ID

From the Device:

- Browser Headers
- Hostname
- Remote IP
- IP (Hashed)
- Port number
- Installed languages
- Default language
- Encoding details
- Accepted Charset
- Source (Facebook, Google Ads, Bing Ads)
- Type of device (Desktop, TV, Tablet, Mobile, Other)
- Timezone

From the device Location:

- Country code
- Region
- Hostname
- City
- Timezone
- Longitude (5km)
- Latitude (5km)

From the ISP

- ISP Name
- ISP Hostname
- ASN

External enriched data:

Device:

- Browser details
- Mobile device brand
- Mobile device type
- Mobile Connection (Yes/No)
- Type of device (Desktop, TV, Tablet, Mobile, Other)
- Timezone

Location:

- Country code
- Region
- City
- Timezone
- Longitude (5km)
- Latitude (5km)

ISP

- ISP Name
- ISP Hostname
- ASN

Fraud signals:

- Darkweb user (yes/no/unknown)
- Known before (yes/no/unknown)
- Trusted (yes/no/unknown)
- Fake user (yes/no/unknown)
- Server (yes/no/unknown)
- Residential ip (yes/no/unknown)
- Company ip (yes/no/unknown)
- Mobile Device (yes/no/unknown)
- VPN (yes/no/unknown)
- Active VPN (yes/no/unknown)
- Datacenter (yes/no/unknown)
- Tor (yes/no/unknown)

- Opera user (yes/no/unknown)
- Abuse network (yes/no/unknown)
- Virusscanner (yes/no/unknown)
- Bot (yes/no/unknown)
- Scraper (yes/no/unknown)