

# InZynk Statement on (GDPR)

InZynk works across the continent but specifically in EMEA and North America, and we have access to data from each such market. Since we have established a strategic partnership with Digital Envoy, which is a data company, we also have access to a large commercial database with up-to-date information on 99% of the global B2B IP space.

InZynk is a B2B marketing services provider, which leverages data based on the IP registered to organizations to leverage their mechanisms associated with core analytics and targeting. According to GDPR, an IP address is defined as Personal Identifiable Information (PII) in case one can leverage it for the identification of an individual.

In relation to this, it is crucial to note that the targeting and analytics capabilities of InZynk do not leverage this data for monitoring or identifying people. It is important to note that InZynk exclusively makes use of IP-data on a company level to facilitate targeting and analytics; hence it is not possible for InZynk to identify an individual and, therefore, doesn't fall under EU Personal Data.

## 1. InZynk's definition of IP-data

If an Internet Service Provider (ISP) owns IP data, it is categorized as EU Personal Data. The European Court of Justice, which is the EU's Highest Court, has clearly defined this:

*In the year 2016, the CJEU clarified the dynamic IP addresses status with respect to the Patrick Breyer v Germany (C-582/14), by stating that an IP address is considered to be personal data if an ISP holds it, without compromising personal data when a party without the "means likely reasonably to be used to identify the individual" holds it.*

With InZynk, IP-data is matched on an organizational level, as opposed to an individual level, and thus, does not have "means likely reasonably to be used to identify the individual."

- a. It is not possible for InZynk to find any individual using merely organizational level IP-data
- b. The IP-data used by InZynk remains anonymous, because of the fact that it is aggregated on an organizational level
- c. InZynk entails no extra data points and does not possess the means or the interest for the identification of individuals based on IP-addresses.

## 2. InZynk acquisition of organizational IP-data

Organizational IP data is procured by InZynk from several vendors. Every vendor was vetted to ensure optimal compliance

- a. The vendors primarily obtain their data from the ICANN "who-is" database. To gain entry into this database, it is necessary to have an active opt-in <https://whois.icann.org/en>.
- b. The systems of InZynk have been built for the retrieval of the updated data from such sources to make sure that the data entails just organizations that managed to opt-in.

### **3. InZynk use cases of IP-data**

#### Use case 1: website analytics

InZynk obtains the permission of the customer to deploy a tracking script on the website of the customer. This javascript interacts with InZynk's systems at each page load.

With this script, the IP address of the visitor is submitted to the system of InZynk, and the main objective is to answer this particular query: Is this a known organization, yes/no? When "yes" is chosen, the event is stored and added to the analytics data of the customer. It is crucial to note that in this reverse IP-lookup, the output that is stored in the analytics of the customer is the organizational domain and organizational name of the visitors as opposed to the IP address.

If the visit data remains unmatched, which is "no" to the question related to a known organization, the reporting and the storing of the event is labelled as unknown. Further actions are not required to identify the visitor.

#### Use case 2: account-based advertising

With InZynk, a targetable segment is created of known organizational IP addresses from its databases. Such a segment is loaded into the Demand Side Platforms (DSPs) connected to InZynk, similar to any other programmatic targeting capabilities that are commonly used.

Subsequently, InZynk purchased advertising directed towards such known segments. InZynk obtains advertising analytics from an aggregated organizational level from the DSPs. Such data can be found and aggregated with the analytics data of a website on an organizational level. The data that is procured from the DSPs does not offer InZynk information enabling the identification of an individual. The data is stored and assessed on an organizational level.

### **4. The exchange of data between InZynk and its customers**

The business objective of InZynk is to ensure that its customers are provided with insights related to the way in which their B2B targeted organisations interact with its marketing content: present on their web page or advertising campaign

- a. Customer input to InZynk: the customer will offer InZynk a list of organizations that they wish to advertise towards, and/or monitor on their webpage
- b. InZynks output to a customer: (i) aggregated web visit data, as well as advertising data from the named organizations provided by the customer. (ii) Further visit data from identified organizations directed towards the website of the customer
- c. No data is exchanged between InZynk and its customers with IP-data. The data identification is related exclusively to either (i) an organizational domain (example: inzynk.com) and/or (ii) an organizational name (example: InZynk ASA)