General Information

When you use GP One services, you entrust us with personal and confidential information, among other things. This privacy policy explains what data we collect, how this data is processed, and why we need this data.

Resonsible

The entity responsible for processing personal data (according to Art. 4 No. 7 DSGVO) is, unless otherwise stated:

Managing Director: Sascha Kalabuchow
GP-One GmbH
Zur Linspher 3 35108 Allendorf (Eder)
+49 6452 911360

Information we collect

The information we collect is used, among other purposes, for analyzing fraud, analyzing website usage concerning advertising spaces, measuring the visibility of advertisements, and/or content areas of websites. Data collection is carried out in accordance with Art. 6 para. 1 f DSGVO to protect our legitimate interests.
Data we collect through the use of our services:

- **Geographical Information**
  Through IP, browser, and/or app, we collect approximate geographical location to verify the correct geographical delivery for the customer.
- **Device Information**
  We collect device-specific information, including GPU, browser, operating system, and the device itself (smartphone, tablet, notebook, car, TV, etc.)
- **Log Data**
  - Details of how you used something in relation to each analysis. This can include the use of a website, watching a video, or viewing an advertisement.
  - IP address (pseudonymized)
  - Browser-specific information such as language, MIME types, plugins, toolbars, extensions, compatibility, version, and status.
  - Unique user tracking, which identifies you uniquely.
- **Cookies, Local Storage, and Similar Technologies**
  - We use various technological methods to recognize a user repeatedly.
  - We operate Ad View tracking without cookies.

Processing of Collected Data

The collected data is used for the following purposes:

- Fraud detection
- Usage analysis
- Visibility assessments
- Fraud protection for customers, agencies, and consumers

The processing of data is carried out in accordance with Art. 6 para. 1 f GDPR to protect our legitimate interests.

Storage Duration

All data is stored for approximately 3 months, with data such as IP addresses immediately anonymized using a hash. Data storage occurs in accordance with Art. 6 para. 1 f DSGVO to protect our legitimate interests.

Information we share

GP-One GmbH does not share personal data with companies, organizations, or individuals except in the following circumstances:

- **With your consent**

  Personal data is only shared with companies, organizations, or individuals outside GP-One GmbH if we have obtained your consent (in accordance with Art. 6 para. 1 a GDPR). Your explicit consent is required for the transmission of any sensitive categories of personal data.
- **For Legal Reasons**

  GP-One GmbH only shares personal data with companies, organizations, or individuals if it is deemed necessary that access to this data or its use, storage, or disclosure is reasonably required:
  - To comply with applicable laws, regulations, or legal processes or respond to enforceable governmental orders. (in accordance with Art. 6 para. 1 c DSGVO)
  - To enforce applicable terms of use, including investigating potential violations. (in accordance with Art. 6 para. 1 f DSGVO)
  - To prevent or address fraud, security vulnerabilities, or technical issues. (in accordance with Art. 6 para. 1 f DSGVO)
  - To protect the rights, property, or safety of GP-One GmbH or the public, as permitted or required by law. (in accordance with Art. 6 para. 1 c and f DSGVO)
- **For processing by other entities**

  Your personal data will only be shared with our partners, other trusted companies, or individuals if we have contracted them to process this data (in accordance with Art. 28 DSGVO).

The confidentiality of all personal data is ensured if GP-One GmbH is involved in a corporate merger, acquisition, or sale of assets. Affected users will be informed in advance before personal data becomes subject to a different privacy policy.

Data security

We make great efforts to protect data from unauthorized access, alteration, disclosure, or destruction.
To protect against unauthorized access to our systems, we regularly review our data collection, storage, and processing practices, including physical security measures. Access to personal data is restricted to employees and contractors of GP-One GmbH who need to know or process it. They are subject to strict confidentiality obligations, the violation of which may result in disciplinary action up to termination of employment.
We encrypt many of our services using SSL.

Scope of the privacy policy

Our privacy policy applies to all services provided by GP-One GmbH and its affiliates. Services offered by other companies or individuals, including products or websites that may include GP-One GmbH services, are not covered by our privacy policy.

Compliance with regulations

Compliance with our privacy policy is regularly reviewed. Upon receiving formal written complaints, we contact the complainant to address the complaint. If we are unable to resolve a complaint regarding the transmission of user data, we cooperate with relevant regulatory authorities, including local data protection authorities.

Changes

Our privacy policy may change from time to time. If changes occur to the privacy policy, they will be published on our website.

Data subject rights

You have the right to access information about the processing of your personal data (in accordance with Art. 15 DSGVO), the right to data portability (in accordance with Art. 20 DSGVO), as well as rights to rectification (in accordance with Art. 16 DSGVO), deletion (in accordance with Art. 17 DSGVO), restriction of processing (in accordance with Art. 18 DSGVO), and/or objection to processing (in accordance with Art. 21 DSGVO) as well as the right to lodge a complaint with a supervisory authority.

Special Information on the Product "GSI"

Storage of IPs in non-human requests
If the IP does not belong to a person but to a data center (crawler, bot, scraper, etc.), the IP is stored in plain text and entered into a database. This information is then compared with the IP registrars of the respective country and permanently stored in our database upon confirmation.

Reason for this exception
Any advertising requests made by non-human actors are considered fraud. This database serves to protect advertisers and website operators.

Transmission of Unique Identifiers (personalized keys)
We do not transmit UIs to our customers via APIs or similar technologies.

Opt-out
We offer you two options for opting out. This prevents us from storing personal information such as Unique Identifiers about you. The opt-out options are available at https://www.gsi-one.org.

- Option 1: Standard Opt-Out
  - In this option, you set a cookie in your browser that informs us that you do not wish to be recognized, and you do not want us to store Unique Identifiers about you. If you delete this cookie, you must perform the standard opt-out again.
  - We use a temporary storage buffer to collect data until it is actually stored. After approximately 30 minutes, the buffer is emptied, and all Unique Identifiers in opt-out-marked data records are deleted.
- **Option 2: Extended Opt-out for fixed IP addresses**
  - If you have a fixed IP address, you can contact us to have this fixed IP address excluded.
  - Recognition via this method is 100% IP-based. If you use VPN, proxy, Tor, or other IP-masking techniques, this opt-out process becomes ineffective.
  - We require information about the contract duration of your internet connection.
  - At least one month before the contract ends, we need a letter from your internet provider confirming that the contract has not been terminated and will continue until a specified date.
  - If we do not receive such a letter in time, the "Extended Opt-Out Process" will automatically expire the day after the contract ends.