

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 it.

Responsible party

Subject to any deviating information, the following party is responsible for the processing of personal data (in accordance with Art. 4 (7) GDPR):

Managing Director: Sascha Kalabuchow
GP-One GmbH
Otto-Wickenhöfer-Str. 7a
35108 Allendorf (Eder)
+49 6452 911360

Information we collect

- **Geographical information**
We use IP, browser, and/or app data to determine the approximate geographical location of the customer in order to verify the correct geographical delivery.
- **Device-related 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 the respective analysis. This may be the use of a website, watching a video, or viewing an advertisement.
 - IP address (pseudonymized)
 - Browser-specific information such as language, MIMEs, plugins, toolbars, extensions, compatibility, version, and status.
 - Unique user tracking, which uniquely identifies you.
- **Cookies, local storage, and similar technologies**
 - We use purpose-built cookies and other technological options to recognize a user repeatedly.
 - We set a technically necessary cookie for opt-out.
 - We work without cookies for ad view tracking.

Legal basis

Based on Art. 6 (1) (f) GDPR (legitimate interest; Recital 47: fraud prevention):

- Fraud detection
- Protection against fraud for end customers, agencies, and end users

Based on Section 25 (2) TTDSG (absolutely necessary)

- Detection of the set opt-out

On the basis of Art. 6 (1) (a) GDPR (consent)

- Usage analyses
- Visibility evaluations

Storage period

All data is stored for 90 days, whereby data such as IP addresses are made unreadable directly by hashing. Storage is carried out in accordance with Art. 6 (1) f GDPR to protect our legitimate interests.

Information disclosed by us

GP-One GmbH does not disclose personal data to companies, organizations, or individuals except in one of the following circumstances:

- **With your consent**
Personal data will only be disclosed to companies, organizations, or individuals outside of GP-One GmbH if we have obtained your consent to do so (in accordance with Art. 6 (1) a GDPR). Your express consent is required for the disclosure of any sensitive categories of personal data.
- **For legal reasons**
GP-One GmbH only discloses personal data to companies, organizations, or individuals if it is deemed necessary that access to this data or its use, storage, or disclosure is relevant:
 - To comply with applicable laws, regulations, or legal proceedings, or to comply with an enforceable official order. (in accordance with Art. 6 (1) c GDPR)
 - To enforce applicable terms of use, including investigating potential violations. (in accordance with Art. 6 (1) f GDPR)
 - To combat or prevent fraud, security breaches, or technical problems. (in accordance with Art. 6 (1) f GDPR)
 - To protect the rights, property, or safety of GP-One GmbH or the public from harm, to the extent permitted or required by law. (in accordance with Art. 6 (1) c and f GDPR)
- **For processing by other parties**
Your personal data will only be made available to our partners, other trustworthy companies, or individuals if we have commissioned them to process this data (in accordance with Art. 28 GDPR).

We guarantee the confidentiality of all personal data in the event that GP-One GmbH is involved in a merger, acquisition, or sale of assets. Affected users will be informed in good time before personal data becomes subject to the provisions of another privacy policy.

Data security

We make every effort to protect data from unauthorized access and from unauthorized modification, disclosure, or destruction.

To protect against unauthorized access to our systems, we regularly review our practices for collecting, storing, and processing data, including physical security measures.

Access to personal data is restricted to employees and contractors of GP-One GmbH who have a compelling need to know or process it. They are subject to strict confidentiality obligations, and failure to comply with these obligations may result in disciplinary action, up to and including 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 affiliated companies. 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. As soon as we receive formal written complaints, we contact the person concerned to deal with the complaint. In the event that we are unable to resolve a complaint about the transfer of users' personal data, we work with the relevant regulatory authorities, including local data protection authorities.

Changes

Our privacy policy may change from time to time. Should any changes be made to the privacy policy, we will publish these changes on our website.

Rights of data subjects

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

Separate information about the “GSI” product

Storing IPs for non-human visits

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 added to a database. This information is then compared with the IP registrars of the respective country and, if confirmed, permanently stored in our database.

Reason for this exception

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

Sharing of unique identifiers (personal keys)

We do not transmit UIs to our customers via APIs or similar technologies.

Essential security/anti-fraud cookies (without consent)

We use purpose-built cookies to detect abuse and invalid traffic (IVT) and to protect the integrity of our advertising transactions. The legal basis is Art. 6 (1) lit. f GDPR (legitimate interest; Recital 47: fraud prevention). The cookies serve security purposes, are not used for advertising, reach measurement, or profiling after the opt-out cookie has been set, and have storage periods of up to 90 days. You can object to the processing at any time in accordance with Art. 21 GDPR. We store your opt-out in an opt-out cookie, which is technically necessary (according to § 25 (2) TTDSG).

Opt-out

We offer you two options for opting out.

This prevents us from processing personal information for purposes other than essential security and anti-fraud measures.

You can find the opt-out options at <https://www.gsi-one.org/en/opt-out.html>

- **Option 1: Standard opt-out**
 - With this option, you set a cookie in your browser that tells us that you do not want to be recognized and that you do not want us to store your unique identifier. Once you delete this cookie, you will need to perform the standard opt-out procedure again.
 - We use temporary storage to collect data until it is actually saved. After approximately 30 minutes, the temporary storage is emptied, the data is read, and any unique identifiers in data records marked for opt-out are deleted.
- **Option 2: Extended opt-out for fixed IP addresses**
 - If you have a fixed IP address, you can contact us and have this fixed IP address excluded.
 - This method relies entirely on your IP address for detection. Therefore, if you use VPN, proxy, Tor, or other IP obfuscation techniques to access the internet, you will render this opt-out process ineffective.
 - We receive information from you regarding the contract term for your Internet connection.
 - No later than one month before the end of the contract, we require a letter from your internet provider stating that the contract has not been terminated and will continue until a specific date.
 - If we do not receive such a letter in time, the “extended opt-out process” will automatically expire on the day after the contract ends.