# Kipy Watch Privacy Policy

The administrator of your personal data is **Kidi Communications Ltd**, headquartered in Israel, Halutzei Hataasiya 2 St., 83815 Kiryat Malachi, tax identification number (TIN): 515847457 ("Kidi Communication", "we", or "us").

The software and related services ("our services" or "Services") provided to the user concern the User's application, called "Kipy Watch". The Kipy Watch application is the property of Kidi Communication and is supported by us, including basic functions such as location requests, video calls, chat messages, remote device management, personalized recommendations, posting messages, interactive communication, as well as other functions within our services.

Kidi Communication understands the importance of users' personal data and will protect it in accordance with applicable laws and Polish regulations. We have prepared this Privacy Policy ("this policy" or "Privacy Policy"), and we especially recommend that you carefully read and understand this policy before using Kipy Watch and related services ("our services"), so you can make informed choices.

**This Privacy Policy will help you understand that:**

- We collect and use your information in accordance with the principles described in this Privacy Policy.
- Data will not be collected in a way that forces the sale of products/services unless you consent to this policy.

When you use our services and enable certain functions, we collect and use the information necessary to provide those functions and services. You may refuse to provide information, but then you may not be able to use certain features or services, unless the information is necessary to perform essential business functions or required by law and regulation. This Privacy Policy specifies when this is the case.

If your account is not logged in, we guarantee the basic function of transmitting information using the device's identification data. If the user logs into their account, the transmission of information will then be based on account information.

Contacts, precise geographical location, cameras, microphones, and permissions to access photo albums are not enabled by default. They are only activated when you authorize their use for specific functions or services. You may revoke this authorization at any time. We do not collect information about you if the relevant function or service is not required, even if we obtained sensitive data with your consent.

This Privacy Policy applies to access and use of our services through the Kipy Watch application, the Kipy Watch software development kit (SDK), and the application programming interface (API) for websites and third-party applications.

This document also defines the Privacy Policy of the KidizWatch store, which in particular includes regulations regarding the protection of personal data in the course of using the services, as well as the security of data entered by the User. The Privacy Policy is an integral appendix to the Terms of Service and Conditions of Use.

The following content will help you understand in more detail how we collect, use, store, process, share, disclose, transmit (if applicable), and protect your personal data. It will also help you understand your rights to access, delete, correct, and withdraw personal data that you have authorized. **Important provisions concerning your personal data are highlighted in bold font, please pay special attention to them.**

**This Privacy Policy explains:**



## 1. How we collect and use personal data

We collect information that you provide directly when using the Services:

### 1.1 Registration, login, authentication

#### 1.1.1 Registration and Login

a) To create an account, during registration and login to our services you must provide the appropriate online identification information (avatar, nickname, password). You may also add your gender, date of birth, region, and personal profile. At the same time, we will store your preferences and account settings.

b) You may also use a third-party account to log in and use the Kipy Watch application. In that case, you authorize us to obtain public information (avatars, nicknames, and other information you authorize) registered on the third-party platform in order to link it with your Kipy Watch account, so that you can log in directly and use our services.

---

### 1.1.2 Authentication

When using a feature or service requiring authentication (Parent or Guardian), in accordance with applicable laws and regulations, **it may be necessary to provide true identity information (phone number) or an appropriate certificate (psychologist's qualification) to complete verification.**
This information is considered sensitive personal data. Refusal to provide it may affect your ability to fully use some functions and services.

---

### 1.2 Browsing Information

a) Kipy Watch may recommend information you may be interested in, and we may collect the necessary login information to provide such functions.

b) Login information used to display information includes:

- Actions taken by the user while using the services: clicks, tracking, favorites, searches, browsing, sharing, and more.
- Information you provide on your own initiative: opinions, posts, likes, comments.
- Geographical information: data from sensors such as GPS, Wi-Fi hotspots, Bluetooth, and base stations.

c) The above information we collect and use is stripped of identification data, and data analysis is only carried out on de-identified, anonymized information that is not directly linked to your identity or associated with your real identity.

---

### 1.3 Function and Interaction

### 1.3.1 Function

a) When using functions related to sending photos, WeChat, and video chat, you will be asked to authorize the use of your camera, photos, and microphone.
**If you refuse, you will not be able to use this function, but it will not affect normal use of other functions.**

b) When using the “SIM IoT card” or real-name authentication functions, in accordance with applicable laws and regulations, you must verify your identity using **facial recognition**. In this process… (continues).

A Third-Party Certification Agency **requires the provision of your real name, identification number, and facial recognition data.**
This information is considered sensitive personal data, and you may refuse to provide it without affecting normal use of other functions.
Such information is used exclusively for authenticating your real name in accordance with applicable laws and regulations, and it will not be used for other purposes without your explicit consent.

---

### 1.3.2 Information Related to Publications

a) When you post content, comments, questions, or answers, we collect information about your posts and display your pseudonym, avatar, or other published content.

b) **When you publish a post and select a display location, we may ask for authorization of permissions related to geographic location. We will collect location information connected to this service. If you refuse to provide precise information about your geographical position, you will not be able to use this function, but this will not affect normal use of other functions.**

c) We also collect information you provide during use of our services (such as comments, messages, graphic posts, audio, and video files).

---

### 1.3.3 Interactive Communication

a) When you actively follow and interact with contacts and groups that interest you, or when you browse, comment, collect, share, like, or forward content, we collect data about the accounts you follow and show you content you may be interested in.

b) **When adding contacts through the Phonebook function, we will ask for your consent to add contacts, and we will encrypt address book information using an encryption algorithm. Information about contacts is treated as confidential personal data. Refusal to provide this information will only prevent the use of the quick add function, but it will not affect the use of other KidizWatch features.**

---

### 1.4 Search

When you use the search service in SeTracker, we collect information about keywords and search logs. To provide you with effective search functionality, some of

this information may be temporarily stored on your local device and displayed as search history.

---

### 1.5 Safe Use

#### 1.5.1 Security Functions

Our main goal is to ensure that you have a safe, trustworthy product and environment, as well as to provide you with high-quality and reliable services. Information collected is used only as necessary to ensure security features.

#### 1.5.2 Device Information and Log Information

a) To ensure the safe operation of software and services, we collect the device model, operating system version number, international mobile equipment identity (IMEI), unique device identifier, hardware address of the network device, IP address, Wi-Fi access point, Bluetooth, base stations, software version number, network access method, type, status, network quality, operation, usage, and service log data.

b) To prevent malicious programs and ensure secure operation, we collect information about installed applications or running processes, general operation of applications, usage and frequency, application crashes, general installation data, performance data, and source of applications.

c) We may use information about your account, device, or service log, as well as other information, which may be used by our branches and partners to determine account security, authentication, detect and prevent security incidents, where you are lawfully authorized to have such access.

---

### 1.6 Changes in the Collection and Use of Personal Data

Please note that as our business develops, we may make changes to the functionality and services we provide. As a rule, when new functions or services are related to existing functions/services, the personal data collected and used will be directly or reasonably related to the primary purpose of processing. If we collect and use your personal data in situations where there is no direct or reasonable connection to the original purpose, we will notify you again and obtain your consent.

---

### 1.7 Exemption from the Requirement of Obtaining Consent for the Collection and Use of Personal Data

Please understand that, in accordance with applicable laws, regulations, and relevant national standards, we may collect and use your personal data without your consent in the following circumstances:

a) Directly related to national security, national defense, or public safety.
b) Directly related to public security, public health, or significant public interests.
c) Directly related to investigation, prosecution, court proceedings, or execution of judgments.
d) For the protection of personal data of the data subject or others, such as life, property, or other major legal rights and interests, where it is difficult to obtain the consent of the individual.
e) Where the data collected is made public by the data subject.
f) Data collected from publicly disclosed information in accordance with the law, such as legal press releases or disclosures by the government.
g) Data necessary to enter into or perform a contract at the request of the user.

h) Necessary for maintaining the safe and stable operation of software and related services, such as detecting and removing software failures.
i) Necessary for providing legal information.
j) Necessary for conducting research by academic institutions or statistical organizations in the public interest, provided that data containing personal information is removed from the results, and the results of academic research or descriptions are publicly disclosed.
k) Other situations required by law and regulations.

**Please note that if information cannot be individually identified or linked with other information, it does not belong to a user's personal data under the law.** If we can or will be able to use data that cannot be linked to any specific personal information in combination with other personal data, it will be treated and protected as personal data in accordance with this Policy during such combination.

---

### 1.7 Payment Information

In the case of payment transactions, data such as: name, surname, card number, expiration date, phone number — is collected.
This data is used solely to complete transactions and is not stored by us.

---

## 2. Additional Information Regarding Consent to Data Use

Below is a short description of permissions that may be used by functions related to the Kipy Watch program.

### 2.1 Permissions for the Phonebook

Functions using this permission: phonebook, importing contacts from address lists.

### 2.2 Permissions for Calls

Functions using this permission: calling function.

### 2.3 Permissions for Location

Functions using this permission: map function, mail function, personal center profile settings.

### 2.4 Permissions for Cameras

Functions using this permission: QR code scanning, photo and video function, personal center profile picture setting, device information settings.

### 2.5 Permissions for Albums

Functions using this permission: remote photo-taking, chat (sending pictures), screen saver settings, posting functions.

### 2.6 Permissions for the Microphone

Functions using this permission: voice reminder function, chat function, video calling function.

---

## 3. Additional Information Regarding the Use of Third-Party Access Rights (SDK / API / H5)

To provide you with a better experience, we will have access to high-quality third-party services. We will carefully evaluate the purpose of using shared information by our partners, conduct comprehensive security assessments, and require compliance with cooperation agreements and legal provisions.
We will strictly monitor the security of software development tools (SDK), application programming interfaces (API), and H5 services to protect data security.

Sharing personal data with third parties requires your explicit consent, unless the data provided is anonymized and cannot be linked to your identity. If a third party needs to use personal data beyond the originally agreed purpose, they must obtain your consent again.

---

### 3.1 Partner Advertising (SDK)

The following permissions are required:
a) Obtaining carrier information;
b) Access to Wi-Fi network information;
c) Reading the current status of the phone;
d) Access to network permissions;
e) Writing/reading data from external mass storage devices;
f) Location;
g) Installation;

h) Obtaining task information;
i) Power management system.

---

### 3.2 Mobile Payments (SDK)

The following permissions are required:
a) Network access;
b) Obtaining network status;
c) Accessing Wi-Fi network status;
d) Reading current phone status;
e) Writing data to internal storage;
f) Writing data to external mass storage devices;
g) Modifying sound settings.

---

### 3.3 Push System (SDK)

The following permissions are required:
a) Network access;
b) Writing to external mass storage devices.

c) Obtaining network status;
d) Obtaining Wi-Fi network status;
e) Reading the current status of the phone;
f) Installation;
g) Obtaining task information;
h) OPPO mobile phone notification (only for OPPO phones);
i) MEIZU mobile phone notification (only for MEIZU phone models).

---

### 3.4 Video Call (SDK)

The following permissions are required:
a) Camera activation;
b) Checking network status (e.g., whether the network can be accessed);
c) Modifying sound settings;
d) Recording;
e) Network access;
f) Writing to external mass storage devices;
g) Obtaining network status;
h) Obtaining Wi-Fi network status;
i) Reading current phone status;
j) Reading external storage devices;
k) Wake lock.

### 3.5 Himalayan (SDK)

The following permissions are required:
a) Writing to external storage devices;
b) Network access;
c) Recording;
d) Obtaining network status;
e) Obtaining Wi-Fi network status;
f) Using the notification service at reception;
g) Camera.

---

### 3.6 Fengfeng School (H5)

The following permission is required:
a) Permission to synchronize encrypted task data.

---

## 4. How We Use Similar Technologies, Such as Cookies

Cookies and similar technologies are widely used on the Internet. When you use our services, we may use these technologies to send one or more cookies or anonymous identifiers to your device to collect and store information about access to and use of Kipy Watch.
We ensure that we do not use cookies for purposes other than those described in this Policy.
We use cookies and similar technologies primarily to achieve the following functions or services:

---

### 4.1 Ensuring the Safe and Efficient Operation of Products and Services

We may set a cookie or anonymous identifier for authentication and security, to allow us to confirm whether the user is safely logged into the Service or has become a victim of theft, fraud, or other violations.
These technologies also help improve the performance of services as well as login and response times.

---

### 4.2 Helping with Easier Access to Data

The use of such technologies may help you avoid steps and processes related to filling out personal data and entering search queries (e.g., search records, form completion).

### 4.3 Recommending, Presenting, and Delivering Content or Accounts You May Be Interested In

We may use cookies and similar technologies to learn about your preferences and usage, and then analyze this data to improve our services, recommend relevant features, information, and content, and optimize advertising.

---

### 4.4 Clearing Cookies

Most browsers and mobile applications provide users with the option to clear stored data. You may clear cookies in your browser or application settings.
If you do this, you may not be able to use certain services or related features offered by Kipy Watch that rely on cookies.

---

## 5. How We Share, Transfer, and Publicly Disclose Personal Data

### 5.1 Sharing

#### 5.1.1 Sharing Principles

a) **Principle of Authorized Consent:** Sharing of your personal data with our affiliates and third parties will only occur with your consent, unless the shared data is anonymized and cannot be linked to your identity. If third parties need to use information beyond the scope originally agreed, they must obtain your consent again.

b) **Principle of Legality and Necessity:** Data shared with affiliates and third parties must serve lawful and legitimate purposes, and only the minimum data necessary to achieve the purpose may be shared.

c) **Principle of Security and Caution:** We will carefully evaluate the purpose of using shared information by third parties, conduct comprehensive security assessments, and require compliance with security measures and cooperation agreements.
We will strictly monitor the security of third-party software used by partners.

#### 5.1.2 Information Shared to Provide Functions or Services

a) We will share anonymized personal data with our affiliates and third parties when you use functions provided by third-party suppliers, such as software providers, intelligent device suppliers, or system service providers, who work with us to provide services on your behalf.
We may also conduct statistical analysis and performance monitoring to recommend

functions and preferences, and deliver more relevant functions, services, or advertising to you.

b) **Third-party account login:** When you use Kipy Watch to log into a third-party product or service, we will provide your pseudonym, profile picture, and other information you authorize to the third-party company, so you can log in.

c) **Location services:** When users use location-related services, we may share location information with third-party providers such as AutoNavi. GPS data is considered sensitive personal data; if you refuse, it will only affect location-related services, while other features will still function.

d) **Payments:** Payment functions are handled by external payment agencies. Such agencies may require you to provide your **name, type and number of your bank card, expiration date, and phone number. Bank card numbers, expiration dates, and phone numbers are sensitive personal data.**
These details are necessary only for completing the payment process. **If you refuse to provide them, only the payment function will be affected — other services will still work.**

---

### 5.1.3 Advertising Control and Analysis

a) **Push Ads:** We may share information with partners responsible for advertising and promotion. However, we do not share identifying information (name, phone number). We only provide anonymized tags or statistics, enabling effective ad delivery without identifying the user.

b) **Statistical Analysis:** We may share statistical data (non-identifiable) with third-party providers to help analyze and measure service performance and advertising effectiveness.

---

### 5.1.4 Sharing Information for Protection and Analysis

a) **User Security:** We take your security seriously. We may share necessary equipment, information, or registration data with partners to protect your account and property rights, preventing violations of your legal rights and interests.

b) **Product Usage Analysis:** To analyze the use of our services and improve user comfort, we may share statistical data about product usage (such as crashes, freezes) with affiliates or third parties. These data cannot identify individuals, but may be combined with other information shared with affiliates or third parties.

---

### 5.1.5 Marketing and Promotion

When you participate in marketing activities organized by us, our affiliates, or third parties, you may be asked to provide information such as your name, address, or contact details.
This information is considered sensitive personal data. If you refuse to provide it, it may only limit your participation in related activities, but other functions will still work. Such data may be shared with affiliates or third parties with your consent to give you a consistent experience during marketing activities.

---

**5.2 Transfers**

a) We will not transfer your personal data to any third party without your explicit consent.

b) In the event of a merger, acquisition, or asset transfer, your personal data may be transferred as part of such activity. If so, we will ensure that the new entity complies with this Privacy Policy and maintains the same or higher security standards.
If this is not possible, we will require the new entity to seek your authorization and consent again.

---

**5.3 Disclosure of Information**

a) We will not publicly disclose your personal information unless required by national laws and regulations or with your consent. In such cases, we will follow industry-standard security practices.

b) **We may disclose important information about your account if penalties are imposed for illegal accounts or fraud.**

---

**5.4 Exemption from Consent for Sharing, Transferring, or Public Disclosure of Personal Data**

Please understand that in the following cases we may share, transfer, or publicly disclose your personal data without your consent, in accordance with applicable laws, regulations, and national standards:

a) Directly related to national security or defense.
b) Directly related to public security, public health, or significant public interest.
c) Directly related to investigation, prosecution, court proceedings, or enforcement of judgments.
d) To protect your or others' life, property, or other significant legal rights, when it is difficult to obtain individual consent.

**6. How We Store Personal Data**

### 6.1 Storage Location

In accordance with legal regulations, we store users' personal data collected and generated during operations in Poland and Germany.
Currently, we do not transfer this data abroad, and if we do, we will comply with applicable national regulations and obtain user consent.
Personal data is stored on servers located in Poland or Germany and is not transferred outside the European Economic Area (EEA).

---

### 6.2 Storage Period

We retain your personal data only for as long as necessary to provide our services: information you post, comments, likes, and related information.
We store and use personal data until the service is terminated or the account is deleted. After that time, we will anonymize your personal data unless otherwise required by law.
Users may request deletion of their personal data at any time. The Administrator may refuse deletion only in cases where storage is necessary due to legal obligations or service settlement and security.

For users whose data must be retained due to legal obligations imposed on the Administrator, or for settlement and security purposes, we will continue to store anonymized data after service termination, but it will only be used for the purpose for which it was originally provided.

---

### 7. How We Protect the Security of Personal Data

a) We take the security of your personal data seriously and will implement appropriate technical and administrative security measures to protect your data from unauthorized access, disclosure, use, modification, damage, or loss.

b) We use encryption, anonymization, and other industry-standard data protection technologies to secure your data, applying security measures no less stringent than those commonly used in the industry, protecting against malicious attacks.

c) We have a professional data security management system, including processes for ensuring data safety and rigorous systems for monitoring access. Only authorized personnel can access your data, and data and technologies are safely controlled in real time.

d) Despite the reasonable and effective measures described above, and the standards required by law, please understand that in the Internet industry it is impossible to guarantee 100% information security at all times.
We will do everything possible to enhance data security, but due to technical

limitations and potential malicious actions, absolute security cannot be assured. Nevertheless, we will make every effort to ensure the safety of your personal data.

e) Please note that communication systems and networks used to access our services may encounter problems caused by factors beyond our control. Therefore, we strongly recommend that you take additional steps to protect your personal data — such as using complex passwords, changing them regularly, and not sharing them with others.

f) We develop emergency plans and activate them in the event of a security incident or data breach to mitigate the impact and consequences.
If such an incident occurs (e.g., data leakage), we will promptly inform you of the nature of the incident, possible consequences, and measures taken or to be taken. We will notify you in an appropriate manner (push notification, text message, or similar).
If individual notification is difficult, we will use reasonable and effective public communication methods.
At the same time, we will report security incidents to relevant regulatory authorities in accordance with legal requirements.

g) When using our services via third-party websites or resources, we are not responsible for protecting your personal data provided to those sites.
Regardless of whether you log in, browse, or use them via links provided by Kipy Watch, please carefully read and follow their privacy protection statements.

---

## 8. Your Rights Regarding Personal Data

We place great importance on managing your personal data and strive to protect your rights to: request access, modification, deletion, withdrawal of consent, authorization, account deletion, submitting complaints regarding privacy functions, and ensuring your ability to protect your privacy and information security.

---

### 8.1 Independent Selection of Personalized Recommendation Information

#### 8.1.1 Independent Control of Receiving Information

**Independent decision-making regarding receiving push notifications:**
Our recommendation features may be based on automated mechanisms, IT systems, and algorithms. During this process, we continuously improve our decision-making to provide you with better services.

We evaluate our recommendation system optimization program with strict auditing strategies.
**In particular, to protect your autonomy in receiving information: if you are not**

**interested in the information we send, or if you want to limit certain recommendations, you may click “X” on the push information bar to block it.**

---

### 8.2 Access, Deletion, and Correction of Personal Data

#### 8.2.1 Accessing Information About Your Personal Account

You may request access to your profile photo, username, gender, date of birth, region, and related information.
You may also update and access this information directly in the Kipy Watch Personal Center – Profile Editing section.

---

#### 8.2.2 Sending Requests, Access, Corrections, Canceling Account Tracking

To make such a request, please contact Customer Service at: kontakt@kipywatch.com, or via our Facebook page.

---

#### 8.2.3 Requests for Access to Collections, Reading Logs, and Search History

To submit such a request, please write to Customer Service using the contact information provided in the previous section.

---

#### 8.2.4 Deleting Published Content

a) Posts, content, or photos you have published may be deleted by pressing the relevant content and clicking the “Delete” button.

b) **Please note: For security and identification reasons, certain information provided during registration, such as mobile phone numbers for recall services, cannot be modified. If you need to update such information, please contact us using the contact details provided in this Policy.**

---

### 8.3 Account Deletion

You may request account deletion by contacting us at: kontakt@kipywatch.com.
Before deleting your account, we will verify your identity and ensure security, including information about your device.
If you request account deletion, we will anonymize your data, unless otherwise required by law.

---

### 8.4 Complaints and Reports

You may file a complaint or report through our information system if you believe your personal data rights have been violated (for example, data collection or usage inconsistent with this Policy).
To do so, please contact Customer Service at: kontakt@kipywatch.com.
We will respond after verifying your identity.

a) You can view this Policy on the home page of the application or on our website: www.kipywatch.com.

b) Please note that the services described in this Policy may differ depending on the device you use — e.g., model, system version, or application version. Ultimately, the services and products you use depend on the software you have installed.

---

### 8.7 Notice of Business Termination

In the event of business termination, we will stop collecting your personal data in a timely manner, notify you of the suspension of services through individual messages or announcements, and delete or anonymize the personal data we hold.

---

### 8.8 Your Rights Regarding Personal Data

In accordance with the provisions of the General Data Protection Regulation (Regulation (EU) 2016/679, “GDPR”), you have the following rights regarding the processing of your personal data:

a) **Right of access to data** – You have the right to obtain confirmation of whether we process your personal data and, if so, to access that data and information about the purpose, scope, and method of processing.

b) **Right to rectification** – You have the right to request correction or completion of your personal data if it is inaccurate or incomplete.

c) **Right to erasure (“right to be forgotten”)** – You have the right to request deletion of your personal data if there is no legal basis for its continued processing.

d) **Right to data portability** – You have the right to receive your personal data in a structured, commonly used, machine-readable format and to request transmission of this data to another administrator.

e) **Right to restriction of processing** – You have the right to request restrictions on the processing of your data in specific cases, e.g., when you contest its accuracy.

f) **Right to object** – You have the right to object to the processing of your data when it is carried out on the basis of our legitimate interests.

g) **Right to withdraw consent** – If processing is based on your consent, you may withdraw that consent at any time. Withdrawal does not affect the lawfulness of processing carried out before the withdrawal.

---

**9. Terms of Service Use by Minors**

a) If you are under 18 years of age, before using our services you should read and accept this Privacy Policy under the supervision and guidance of your parent or legal guardian.

b) We protect minors' personal data in accordance with applicable Polish laws and regulations. We will collect, use, store, share, or disclose minors' personal data only in ways permitted by law, with the explicit consent of their parent or guardian.

c) If you are the legal guardian of a minor and have any questions regarding the personal data of the minor under your care, please contact us using the contact details provided in this Policy.

---

**10. Changes and Notifications Regarding the Policy / Contact Us**

a) To provide you with better services, our policies will be updated and changed from time to time. We will make timely changes to this Policy, which form an integral part of it and are equivalent to this Policy. Unless otherwise provided, we will continue to protect your rights under this Policy without requiring your explicit consent each time.

b) If we make updates, we will publish the updated version in Kipy Watch before the new terms take effect, and we will provide additional notices (such as pop-up reminders, announcements, or notifications within the Service, or by sending notifications).
We encourage you to review this Policy regularly to stay informed about how we protect your privacy.

---

**11. Cookie Policy**

a) For user convenience, www.kipywatch.com uses cookies, among other things, to customize the service to users' needs and for statistical purposes.
Cookies are small text files stored by your web browser on your device.

b) On www.kipywatch.com, we use two types of cookies:

- **Session cookies** – temporary, stored until the user logs out, leaves the website, or closes the browser.
- **Persistent cookies** – stored on the user's device for a set period or until the user deletes them.

c) On www.kipywatch.com, we use the following types of cookies:

- **Necessary** – enable use of services provided on www.kipywatch.com (e.g., handling authorization).
- **Security** – help ensure service security, e.g., detecting abuse.
- **Performance** – enable the collection of statistics on service usage.
- **Functional** – allow customization of user interface settings, e.g., selected language or region.

- **12. Logs**
- In line with the practice of most websites, we store HTTP requests directed to our server (server logs). As a result, we store:
- a) IP addresses from which users browse the information content on www.kipywatch.com;
  b) time of the request;
  c) time of response;
  d) client station name – identification carried out via HTTP protocol;
  e) information about errors that occurred during HTTP transactions;
  f) URL address of the page previously visited by the user (referrer link);
  g) information about the user's browser;
  h) data collected in log files, used exclusively for administrative purposes of www.kipywatch.com.
- i) The collected logs are stored only for the time necessary to perform user-ordered services, then anonymized and used solely as auxiliary material for website administration.
  The information contained therein is not disclosed to anyone except authorized administrators of www.kipywatch.com.
  Based on log files, statistical summaries may be generated to support administration. These summaries do not contain any identifying data of users visiting the website.
- ---
- **13. Contact Us**
- If you have complaints, suggestions, or questions about personal data protection, you can contact our Customer Service team at: **kontakt@kipywatch.com**, and we will respond promptly.
  You can also visit our website: www.kipywatch.com