1. Introduction

This Privacy Policy ("Policy") explains in detail how **Sole Proprietor Luzhniy Vladyslav Olehovich**, operating under the brand name **GPChat**, collects, uses, stores, shares, and protects your personal and non-personal information when you interact with our products and services, including but not limited to:

- **The GPChat mobile application** ("App"), available for download from official digital distribution platforms such as **Google Play** and **Apple App Store**; and
- **The GPChat website** located at **https://gpchat.co/** ("Website"), along with any associated domains, subdomains, and web services we operate.

This Policy is designed to help you understand your privacy rights, the measures we take to safeguard your data, and the obligations you undertake by using our Services.

By accessing or using the App and/or the Website, you explicitly consent to the practices described herein, including the processing, transfer, and storage of your information as outlined in this Policy. If you disagree with any part of this Policy, you must immediately discontinue the use of our Services.

This Policy complies with the applicable **laws of Ukraine**, the **General Data Protection Regulation (EU) 2016/679 (GDPR)** for European users, and other relevant international data protection frameworks.

We strongly encourage you to review this document carefully. If you have any questions regarding its content, you can contact us using the details provided in **Section 13 (Contact Information)**.

---

2. Information We Collect

We collect various types of information from and about users to provide a safe, efficient, and personalized experience. This includes:

2.1. Information You Provide Directly

We collect information that you choose to provide when you interact with our Services, such as:

- **Account Registration Data:** Name, email address, password, and optional profile details (e.g., profile picture, biography).
- **Billing and Payment Details:** Credit card number, expiration date, billing address, and other necessary payment credentials. These are processed through secure third-party payment gateways; we never store full card data on our servers.
- **User-Generated Content:** Any prompts, text, files, or other data you submit while using the App. This may include AI conversation logs, images, or documents.

- **Customer Support Correspondence:** Records of communications with our support team, including requests, questions, or complaints.

2.2. Information Collected Automatically

When you use our Services, we automatically gather certain data, which may include:

- **Device Data:** Hardware model, operating system version, browser type, IP address, unique device identifiers (UDIDs, IMEIs, MAC addresses).
- **Usage Analytics:** Interaction patterns, session duration, navigation paths, and feature usage metrics.
- **Cookies and Similar Technologies:** Small text files or other identifiers that store your preferences, authentication tokens, and other session-related information.

2.3. Information from Third Parties

We may receive additional data about you from trusted third-party sources, such as:

- **App Stores:** Google Play and Apple App Store may provide us with installation, update, and purchase data for verification purposes.
- **Third-Party API Providers:** If you integrate GPChat with services such as OpenAI, Google Gemini, or Midjourney, we may receive basic account identifiers or usage data from those platforms, in compliance with their respective privacy policies.

All information collected is handled in accordance with this Policy and relevant legal frameworks.

---

3. How We Use Your Information

We process the information collected from you for a variety of legitimate business and operational purposes, always ensuring that such processing is lawful, transparent, and proportional. The key purposes include, but are not limited to:

3.1. Service Delivery and Account Management

- To create, verify, and maintain your user account.
- To process transactions, deliver purchased services or subscriptions, and provide you with access to premium features.
- To personalize your experience by displaying relevant content, suggestions, and interface configurations.

3.2. Improvement and Optimization

- To analyze trends, track user engagement, and identify opportunities to enhance our Services.

- To conduct research and development aimed at improving our AI features, user interface, and overall performance.
- To A/B test new functionalities and measure their impact.

3.3. Communication

- To respond to your inquiries, support requests, or feedback.
- To send service-related announcements such as software updates, changes to our Terms of Service, or policy updates.
- To provide marketing and promotional communications, subject to your consent where required by law.

3.4. Compliance and Security

- To detect, prevent, and investigate fraudulent activities, unauthorized access, or violations of our Terms of Service.
- To comply with applicable legal obligations, regulatory requirements, or lawful government requests.
- To enforce our contractual rights, resolve disputes, and protect the integrity of our systems.

---

4. Legal Basis for Processing Personal Data

Under applicable data protection laws, including the **General Data Protection Regulation (GDPR)** for EU users and Ukrainian privacy legislation, we rely on the following legal grounds to process your personal data:

4.1. Contractual Necessity

We process your personal information where it is necessary to fulfill the terms of a contract we have with you—such as providing the services you have requested or purchased. Without this data, we cannot deliver the Services as intended.

4.2. Consent

In certain cases, we will request your explicit consent before collecting or processing specific types of personal data, particularly for marketing communications, optional analytics, or integration with third-party APIs. You have the right to withdraw your consent at any time without affecting the lawfulness of processing based on consent before its withdrawal.

4.3. Legitimate Interests

We may process your information where it is reasonably necessary to pursue our legitimate interests—such as improving our products, maintaining network security, or preventing

fraudulent activity—provided these interests are not overridden by your fundamental rights and freedoms.

4.4. Legal Obligations

We may be required by applicable laws or court orders to process certain personal data for compliance purposes, including tax reporting, anti-money laundering (AML) checks, and responding to lawful governmental requests.

4.5. Vital Interests

In rare circumstances, we may process your personal data to protect your vital interests or those of another individual, for example in emergency situations where there is a threat to health or safety.

---

5. Data Sharing and Disclosure

We do not sell, rent, or trade your personal information to third parties for their direct marketing purposes. However, we may share your data under the following carefully controlled circumstances:

5.1. Service Providers and Contractors

We may engage third-party vendors, service providers, and contractors to perform business functions on our behalf. These functions include:

- Hosting and infrastructure services.
- Customer support and live chat systems.
- Payment processing and billing services.
- Analytics, monitoring, and performance optimization.

All such third parties are bound by contractual obligations to keep your information secure and to use it only for the purposes specified in our agreements.

5.2. Business Transfers

In the event of a merger, acquisition, sale of assets, bankruptcy, or reorganization, your personal information may be transferred as part of the business assets to the acquiring entity. In such cases, we will notify you before your personal data becomes subject to a different privacy policy.

5.3. Legal Compliance and Protection

We may disclose your information if we believe in good faith that such disclosure is necessary to:

- Comply with a legal obligation, court order, or governmental request.
- Enforce our Terms of Service or defend against legal claims.
- Detect, prevent, or address fraud, security breaches, or other unlawful activities.

5.4. Aggregated or Anonymized Data

We may share aggregated, anonymized data that does not identify you personally with partners, advertisers, or other organizations for research, statistical, or business analysis purposes.

---

6. Data Retention

We retain your personal data only for as long as is necessary to fulfill the purposes for which it was collected, or as required by applicable law. The retention period will vary depending on the nature of the data and the reasons for which it was collected.

6.1. Retention Criteria

- **Contractual data**: Retained for the duration of your relationship with us and for a period thereafter as necessary to comply with legal obligations or to resolve disputes.
- **Marketing data**: Retained until you opt-out or withdraw consent, after which it will be promptly deleted or anonymized.
- **Usage logs**: Stored for operational and security purposes for a limited period, typically not exceeding 12 months, unless required for legal or regulatory purposes.

6.2. Deletion and Anonymization

When personal data is no longer needed, we will securely delete or anonymize it so that it can no longer be linked back to you.

6.3. Legal Exceptions

Certain legal or regulatory obligations may require us to retain specific records for longer periods (e.g., tax records for up to 7 years under Ukrainian law).

7. International Data Transfers

As a company operating in Ukraine and offering services globally, we may process and store your personal information outside of your country of residence, including in the European Union, the United States, or other jurisdictions where our service providers are located.

7.1. Transfer Safeguards

Whenever we transfer your personal information internationally, we take all reasonable measures to ensure that your data is protected in accordance with this Privacy Policy and applicable laws. These measures may include:

- **Standard Contractual Clauses (SCCs)** approved by the European Commission.
- **Binding Corporate Rules (BCRs)** adopted by certain service providers.
- Relying on countries deemed to provide an adequate level of protection for personal data.

7.2. Consent for Cross-Border Transfers

By using GPChat and providing your personal information, you consent to the transfer, storage, and processing of your data in countries outside your own, which may have different data protection rules than those in your country.

7.3. Service Providers Abroad

We ensure that all third-party providers involved in cross-border data processing are contractually obligated to implement robust security measures and to process data only for authorized purposes.

---

8. Data Security

We take the protection of your personal information seriously and have implemented appropriate administrative, technical, and physical safeguards to prevent unauthorized access, use, alteration, or disclosure of your data.

8.1. Technical Measures

- **Encryption in transit and at rest** using industry-standard protocols (e.g., TLS/SSL, AES-256).
- **Secure data storage** in controlled environments with restricted physical access.
- **Network firewalls and intrusion detection systems** to monitor and block malicious activity.

8.2. Organizational Measures

- Access to personal data is restricted to authorized personnel who require it to perform their duties.
- All employees and contractors are bound by confidentiality agreements.
- Periodic security training for staff to maintain awareness of data protection practices.

8.3. Incident Response

In the event of a security breach that affects your personal data, we will:

1. Take immediate steps to contain the breach and mitigate potential harm.
2. Notify affected users without undue delay, as required by applicable law.
3. Cooperate fully with regulatory authorities and provide them with relevant information.

8.4. User Responsibility

While we take every reasonable precaution to protect your data, you are also responsible for maintaining the security of your account credentials, avoiding suspicious links, and ensuring that your devices are protected from malware.

9. Your Rights

Depending on your location and applicable data protection laws, you may have specific rights in relation to your personal information. We respect and facilitate the exercise of these rights to the fullest extent permitted by law.

9.1. Right to Access

You have the right to request confirmation as to whether we process your personal information and, if so, to receive a copy of that information along with details about how it is used.

9.2. Right to Rectification

If you believe that any of the personal information we hold about you is inaccurate or incomplete, you have the right to request corrections or updates.

9.3. Right to Erasure ("Right to be Forgotten")

You may request that we delete your personal information in certain circumstances, such as when it is no longer necessary for the purposes for which it was collected or if you withdraw your consent.

9.4. Right to Restrict Processing

You can request that we limit the processing of your personal data, for example, if you contest its accuracy or object to its use.

9.5. Right to Data Portability

Where technically feasible, you may request a copy of your personal data in a structured, commonly used, and machine-readable format, and you have the right to transmit that data to another controller.

9.6. Right to Object

You have the right to object to the processing of your personal data for specific purposes, including direct marketing or profiling.

9.7. Right to Withdraw Consent

If we rely on your consent for processing, you can withdraw that consent at any time without affecting the lawfulness of processing based on consent before its withdrawal.

---

10. Exercising Your Rights

10.1. How to Submit a Request

To exercise any of the rights described above, you can contact us at:

Legal Entity: FOP Luzhnyi Vladyslav Oleh
Address: Zaporizhske Kozatstvo Street 7, Apt. 15, Zaporizhzhia, Zaporizhzhia Oblast, Ukraine,

69097
Email: support@gpchat.co
Phone: +380955959048

Please provide sufficient information for us to verify your identity before we act on your request. This may include a copy of your government-issued identification document or other relevant proof of identity.

10.2. Timeframe for Response

We aim to respond to all valid requests within one month. If your request is complex or we have received a high volume of requests, this period may be extended by an additional two months.

10.3. Limitations

In some cases, we may not be able to fulfill your request if:

- Doing so would violate the rights of another individual.
- The data is required to comply with legal obligations.
- The request is manifestly unfounded or excessive.

10.4. No Charge for Requests

We do not charge a fee for processing reasonable requests. However, we may charge a fee or refuse to act on requests that are manifestly unfounded, excessive, or repetitive.

---

11. Cookies and Similar Technologies

11.1. What Are Cookies

Cookies are small text files placed on your device (computer, smartphone, tablet) when you visit a website or use an application. They allow us to recognize your device, store your preferences, and improve your user experience.

11.2. Types of Cookies We Use

- **Strictly Necessary Cookies** – Required for the operation of our website and application, such as authentication, security, and load balancing.
- **Performance Cookies** – Help us understand how visitors use our services so we can improve functionality and performance.
- **Functional Cookies** – Allow us to remember your choices, such as language preferences and customized layouts.
- **Targeting and Advertising Cookies** – Enable us to deliver more relevant ads and measure their effectiveness.

- **Third-Party Cookies** – Set by analytics providers, ad networks, or partners that assist us in delivering our services.

11.3. Cookie Duration

Cookies may be **session cookies** (deleted when you close your browser) or **persistent cookies** (remain on your device for a set period).

11.4. Your Cookie Choices

You can manage or disable cookies through your browser settings. Please note that disabling cookies may affect the functionality of certain features of our services.

11.5. Do Not Track

Our website and application currently do not respond to "Do Not Track" signals due to the lack of a consistent industry standard.

---

12. Tracking, Analytics, and Third-Party Tools

12.1. Analytics Services

We use third-party analytics providers, such as **Google Analytics**, **Firebase Analytics**, and similar services, to collect and analyze usage data. These tools help us understand how our services are accessed and used, enabling us to improve features and performance.

12.2. Information Collected by Analytics Tools

These tools may collect:

- Device type, operating system, and browser information.
- IP address (anonymized where required by law).
- Usage data, including time spent on pages, clicks, and navigation paths.
- Geographic location (approximate, not precise GPS unless explicitly granted).

12.3. Third-Party Advertising Networks

We may partner with advertising networks such as **Google Ads** and **Meta Ads** to deliver relevant ads. These networks may use cookies, tracking pixels, or SDKs to personalize advertising content and measure campaign performance.

12.4. Social Media Plugins and Widgets

Our services may include social media features such as "Share" or "Like" buttons. These features may collect your IP address and set cookies to function properly. Interactions with these features are governed by the privacy policies of the respective platforms.

12.5. Disabling Tracking

Most browsers and mobile operating systems allow you to control whether cookies or tracking scripts are stored. Some third-party services, like Google Analytics, offer opt-out mechanisms (e.g., Google Analytics Opt-Out Browser Add-on).

---

13. Security & Data Protection

We take the security of your personal data and all user-related information very seriously. GPChat implements and maintains reasonable administrative, technical, and physical safeguards designed to protect your data from unauthorized access, use, modification, disclosure, or destruction. These safeguards are continuously reviewed and improved in accordance with industry standards and applicable legal requirements under the jurisdiction of Ukraine.

Our security measures include, but are not limited to:

- **Encryption in transit and at rest:** All sensitive information is transmitted via secure HTTPS/TLS protocols and, where applicable, stored in encrypted databases.
- **Access control:** Only authorized personnel with a strict business need have access to your data, and all access is logged and monitored.
- **Regular vulnerability assessments:** We routinely test our infrastructure, APIs, and application code for security vulnerabilities and apply necessary updates or patches immediately.
- **Secure API usage:** GPChat uses third-party APIs (such as those from OpenAI, Google, Apple, and others) in compliance with their official Terms of Service. Data sent to these APIs is minimized to the extent required for functionality, encrypted during transmission, and never used for purposes beyond those explicitly stated in our Terms of Service and Privacy Policy.

When using APIs from third parties (including AI models, natural language processing engines, and image generation services), we ensure that:

1. **All data transfers are secure:** Any user-provided data sent to these APIs is encrypted and handled according to the privacy standards of the API provider.
2. **Data minimization applies:** Only the information strictly necessary for processing is shared.
3. **No unauthorized reuse:** API providers are contractually or legally bound not to use shared data for purposes unrelated to the service requested by GPChat.

While we take every reasonable measure to protect your data, no method of transmission over the Internet or method of electronic storage is 100% secure. As such, we cannot guarantee absolute security, and you acknowledge and accept this risk when using GPChat's services. In

the unlikely event of a data breach, we will notify affected users in accordance with applicable laws and regulations, and will take immediate action to mitigate any possible harm.

---

14. Third-Party APIs & Integrations

GPChat's functionality is enhanced by the integration of multiple **third-party Application Programming Interfaces (APIs)** and platform services. These integrations allow us to deliver advanced features, such as natural language processing, image generation, translation, voice recognition, and other capabilities that would otherwise not be feasible within the scope of our proprietary technology.

The third-party APIs and services we currently utilize (or may utilize in the future) include, but are not limited to:

- **OpenAI API** (for AI-driven text generation and natural language processing)
- **Google APIs** (for analytics, cloud services, and application store distribution through Google Play)
- **Apple APIs** (for application store distribution through the Apple App Store and device-level integrations)
- **Other AI or technology providers** offering specific modules or services that enhance GPChat's performance and usability

All integrations are implemented **in strict compliance** with the Terms of Service, Privacy Policies, and usage restrictions of the respective providers. We never claim ownership of third-party technologies, nor do we misrepresent GPChat as being an official product of any third-party provider. GPChat operates as an **independent product** owned and managed by **FOP Luzhnyi Vladyslav Olehovich**, legally registered in Ukraine.

To maintain transparency and protect user rights, GPChat adheres to the following principles regarding third-party APIs:

1. **Purpose Limitation:** We only connect to external APIs for clearly defined functions described within the GPChat app or website, and never for unrelated data collection or profiling.
2. **Data Minimization:** Any personal or interaction data transmitted to third-party APIs is limited to what is strictly necessary for the requested feature.
3. **Secure Transmission:** All API communications occur over encrypted channels (HTTPS/TLS or equivalent), and we employ additional security layers where possible.
4. **No Unlawful Use:** We strictly prohibit any use of third-party APIs that would violate applicable laws, infringe intellectual property rights, or breach the providers' contractual terms.

5. **User Awareness:** We disclose in our Terms of Service and Privacy Policy that GPChat uses third-party APIs and integrations. Where required by law, we will request explicit user consent before processing any data through these services.

By using GPChat, you acknowledge and consent that certain features of the application may require interaction with these third-party APIs, and that such interactions are essential for the full functionality of the service. While GPChat strives to ensure that all third-party providers maintain high standards of data protection, we are not responsible for the independent practices of those providers. We encourage users to review the Terms of Service and Privacy Policies of these third-party services, which are available on their official websites.

---

15. App Store & Google Play Compliance

GPChat is developed, maintained, and distributed in **full compliance** with the official policies, guidelines, and requirements of the Google Play Store and the Apple App Store. This commitment ensures that our users receive a safe, reliable, and policy-compliant product regardless of the platform on which they choose to download GPChat.

Our compliance practices include, but are not limited to:

1. **Policy Adherence:**
    - We regularly review and update GPChat to align with the most recent versions of the **Google Play Developer Program Policies** and **Apple App Store Review Guidelines**.
    - We maintain internal processes for quickly identifying and resolving potential violations, whether related to content, user data, advertising, or in-app behavior.
2. **Content Compliance:**
    - GPChat does not contain prohibited or restricted content, including but not limited to explicit sexual material, hate speech, excessive violence, or misleading claims.
    - The app interface, marketing materials, and in-app features avoid infringing on the intellectual property rights of any third party, including logos, trademarks, and copyrighted works.
3. **Data Protection:**
    - GPChat strictly complies with the **Google Play User Data Policy** and the **Apple App Store Privacy Guidelines**.
    - All required disclosures regarding data collection, storage, and processing are made within the app listing and in this Privacy Policy.
    - User consent is requested when mandated by applicable law or platform rules.
4. **Accurate Representation:**

- All descriptions, screenshots, promotional images, and videos used in Google Play and App Store listings accurately represent the features and capabilities of GPChat.
- We avoid deceptive or manipulative tactics, ensuring that potential users receive truthful and transparent information before downloading.

5. **Security and Safety:**
    - GPChat undergoes regular security reviews before each app store release to detect and address potential vulnerabilities.
    - We implement measures to prevent the distribution of malware, spyware, or any malicious code within the app package.
6. **App Store-Specific Requirements:**
    - For **Google Play**, we comply with Android-specific permissions, API usage restrictions, and advertising ID rules.
    - For **Apple App Store**, we follow requirements for iOS permissions, app tracking transparency (ATT) disclosures, and in-app purchase compliance.

By downloading GPChat from either Google Play or the Apple App Store, you acknowledge that the application is provided in accordance with the terms set by these platforms. You also agree to comply with their respective user agreements, in addition to GPChat's Terms of Service and Privacy Policy.

---

16. Security Measures and Data Integrity

We take the security of user information and the operational integrity of GPChat extremely seriously. Our security framework is designed to safeguard against unauthorized access, disclosure, alteration, or destruction of data.

1. **Technical Safeguards:**
    - All communications between GPChat and its servers are encrypted using industry-standard **TLS (Transport Layer Security)** protocols.
    - Sensitive data, including authentication tokens and stored user preferences, are encrypted at rest using **AES-256** or an equivalent level of encryption.
2. **Access Controls:**
    - Access to user data within our infrastructure is restricted to authorized personnel only, based on their role and operational necessity.
    - Multi-factor authentication (MFA) is enforced for all administrative accounts that can access production systems.

3. **Ongoing Monitoring:**
    - We employ continuous monitoring solutions to detect unusual patterns of behavior, unauthorized login attempts, or potential data breaches.
    - In case of a suspected or confirmed breach, we follow a documented incident response plan that includes notifying affected users and relevant authorities in compliance with applicable laws.
4. **Regular Security Audits:**
    - Independent security audits and penetration testing are performed periodically by certified third-party providers.
    - Identified vulnerabilities are prioritized and remediated promptly to maintain system integrity.

By using GPChat, you acknowledge and agree that, while we take every reasonable precaution, no online platform can be 100% immune to security risks, and you accept such risks inherent to digital communications.

---

17. Amendments to This Privacy Policy

We reserve the right to amend or update this Privacy Policy at any time to reflect changes in our practices, technological advancements, legal requirements, or other factors affecting the operation of GPChat.

- **Notification of Changes:**
  Whenever material changes are made, we will notify users by updating the "Last Updated" date at the top of this document and, where appropriate, provide a prominent notice within the GPChat app and on our website **gpchat.co**.
- **User Review:**
  It is the responsibility of the user to periodically review this Privacy Policy to stay informed of our practices. Continued use of GPChat after the effective date of any changes constitutes acceptance of the updated policy.
- **Version Control:**
  Previous versions of this Privacy Policy will be archived and made available upon written request, to ensure transparency in our privacy practices.

---

18. Contact Information

If you have any questions, concerns, or requests regarding this Privacy Policy, the practices of GPChat, or your dealings with us, please contact us at:

Legal Entity:
FOP Luzhnyi Vladyslav Oleh
Address: 7 Zaporizkoho Kozatstva Street, Apt. 15, Zaporizhzhia, Zaporizhzhia Region, 69097, Ukraine
Phone: +380955959048
Email: support@gpchat.co

We are committed to responding to all legitimate inquiries within the timeframe required by applicable law, and to resolving privacy concerns in a timely and transparent manner.