Privacy Policy of Pixflame

Last Updated: 2025/09/03

---

1. Introduction

This Privacy Policy ("Policy") explains how **FOP Hrymaliuk Pavlo Ivanovych**, a sole proprietor registered in Ukraine under the Tax Identification Number **3413810710**, operating under the brand name **Pixflame**, collects, processes, stores, and protects both personal and non-personal data of its users.

This Policy governs the use of all services operated by Pixflame, including:

- the **Pixflame mobile application** (the "App"), available for download on Google Play; and
- the **Pixflame website** at https://pixflame.co and its subdomains (the "Website").

By installing or using our App or Website (collectively referred to as the "Services"), you agree to the collection and use of information in accordance with this Policy. If you disagree with any part of it, you should discontinue the use of Pixflame immediately.

Pixflame is committed to transparency, data security, and the protection of user rights. This Policy complies with the laws of Ukraine, the **General Data Protection Regulation (EU) 2016/679 (GDPR)**, and other applicable international privacy frameworks. We recommend that all users read this Policy carefully to understand how their data is handled and what rights they possess.

If you have any questions or requests regarding your data or this Policy, please refer to the contact details provided in **Section 17 (Contact Information)**.

---

2. Information We Collect

To provide and continuously improve our Services, Pixflame collects various categories of information. We always limit collection to what is strictly necessary and process it lawfully, fairly, and transparently.

2.1 Information Provided Directly by You

When you interact with Pixflame, you may provide information voluntarily, including:

- **Account Information:** your name, email address, password, and optional profile details such as username or profile photo.
- **Payment Data:** information related to your subscription or purchase made via Google Play, including payment method and billing details. Pixflame does not store or have access to full credit card numbers.

- **Uploaded Content:** any images or media files you edit, upload, or save within the App.
- **Support Correspondence:** communications sent to our support team through email or the in-app contact form.

2.2 Information Collected Automatically

When you use our Services, certain data is automatically collected to maintain performance and security:

- **Device Information:** such as device type, model, operating system, unique device identifiers, IP address, and language settings.
- **Usage Data:** including app activity, session duration, interactions with editing tools, crash logs, and performance analytics.
- **Cookies and Tracking Technologies:** small data files used on the Website to remember preferences, improve navigation, and ensure smooth user experience.

2.3 Information from Third Parties

We may receive limited information from trusted partners, such as:

- **Google Play Services**, for installation, update, and payment confirmations;
- **Analytics Platforms**, providing anonymized usage insights;
- **Social Media Integrations**, if users choose to share edited photos directly from the App.

Pixflame never purchases user data and only processes third-party information according to this Policy and relevant laws.

---

3. How We Use Your Information

Pixflame processes user information to deliver, enhance, and personalize the Services, ensuring a secure and efficient experience. The purposes of data processing include, but are not limited to:

3.1 Service Operation and Account Management

- To create and manage user accounts, enabling access to free and premium features.
- To process subscription payments and confirm purchases through secure, certified payment processors.
- To synchronize user data and preferences across devices for seamless editing continuity.
- To provide customer support and resolve technical issues.

3.2 Personalization and Product Enhancement

- To tailor the App's interface, filters, and features based on user preferences and behavior.
- To recommend creative tools, effects, or updates that match individual usage patterns.
- To conduct statistical analysis that helps improve functionality, design, and performance.

3.3 Legal, Security, and Compliance Purposes

- To prevent fraud, unauthorized access, and misuse of our Services.
- To comply with legal and regulatory obligations under applicable laws.
- To protect Pixflame's intellectual property, enforce agreements, and ensure a safe environment for users.

Pixflame does not sell or rent personal data under any circumstances. All processing activities are carried out in accordance with the principles of necessity, proportionality, and respect for user rights.

---

4. Legal Basis for Processing Personal Data

Pixflame operates internationally and serves users across different jurisdictions, including the European Union. Therefore, we adhere to both **Ukrainian law** and the **General Data Protection Regulation (GDPR)** when processing personal data. Every action we take with respect to your data is grounded in one or more of the following lawful bases:

4.1 Performance of a Contract

We process your data when it is necessary to provide the services you have requested or to fulfill a contractual obligation between you and Pixflame. This includes creating and maintaining your user account, enabling access to premium features, processing payments, and ensuring that your subscription benefits are correctly applied. Without this data, we cannot deliver essential functionality or support the continued use of your subscription.

4.2 Consent

In some circumstances, we rely on your explicit consent before collecting or processing certain data. Examples include:

- Sending optional marketing messages or promotional emails;
- Collecting analytics data beyond the strictly necessary scope;
- Accessing your camera, photo library, or microphone for editing features;
- Using cookies and tracking tools on our Website.

You can withdraw your consent at any time without affecting the lawfulness of prior processing. Pixflame provides accessible options in both the App and the Website for managing permissions and preferences.

4.3 Legitimate Interests

We may process limited data where it serves our **legitimate interests**, provided these do not override your fundamental rights and freedoms. Legitimate interests include improving security, detecting fraud, maintaining service quality, and developing new features. Pixflame always balances such interests against your right to privacy and transparency.

4.4 Legal Obligations

Certain types of data processing are required to comply with legal obligations — for instance, tax reporting, accounting, or responding to valid requests from authorities. In such cases, we retain only the minimum necessary information and ensure lawful disclosure.

4.5 Vital Interests

In exceptional cases, we may process data to protect your vital interests or those of another individual — for example, in urgent security incidents or cases of suspected identity theft. Such processing occurs rarely and only when absolutely necessary to prevent harm.

Pixflame never processes data for purposes inconsistent with the above. Each processing activity is documented and reviewed regularly to ensure compliance and fairness.

---

5. Data Sharing and Disclosure

Pixflame respects your privacy and treats personal data as confidential business information. We do **not sell, rent, or trade** your personal information to third parties for marketing or profit. However, in certain controlled circumstances, data may be shared to ensure the proper operation of our Services and compliance with the law.

5.1 Service Providers and Technical Partners

We may share limited personal information with trusted third-party providers who perform functions on our behalf, such as:

- **Cloud hosting and data storage services**, which securely maintain user files and account data;
- **Payment processors** (e.g., Google Play Billing), which handle transactions and verify payment details;
- **Analytics services**, helping us understand how users interact with Pixflame to enhance performance;
- **Customer support tools**, enabling efficient management of support requests and feedback.

All such partners are contractually obligated to:

- Use data **only** for the specific purpose assigned to them;
- Maintain **strict confidentiality** and **data security**;
- Comply with GDPR and applicable data protection laws.

We routinely audit these providers to ensure continued compliance and reliability.

5.2 Business Transfers

In the event that Pixflame undergoes a merger, acquisition, corporate restructuring, or asset sale, personal data may be transferred as part of that transaction. Any such transfer will be handled transparently, and users will be notified before their data becomes subject to a new privacy framework.

5.3 Legal Compliance and Protection

We may disclose your personal data where required by law or if we believe in good faith that disclosure is necessary to:

- Comply with legal or regulatory obligations;
- Respond to lawful requests from authorities;
- Protect Pixflame's rights, assets, and intellectual property;
- Prevent fraud, misuse, or security breaches.

Disclosures of this nature are carefully reviewed by our legal team to ensure necessity and proportionality.

5.4 Aggregated and Anonymized Data

We may share aggregated, de-identified data that cannot reasonably be used to identify you. This includes statistical analyses, performance metrics, and anonymized usage patterns shared with research partners or advertisers for insights and service improvement.

Pixflame remains fully accountable for any data shared on its behalf and ensures that all recipients adhere to strict privacy standards consistent with this Policy.

---

6. Data Retention

Pixflame retains personal and non-personal data only for as long as it is necessary to fulfill the purposes outlined in this Policy, comply with applicable laws, or resolve disputes. We do not keep user information indefinitely and periodically review retention schedules to ensure data is stored no longer than required.

6.1 General Retention Principles

- **Account Information:** We retain your account data for the lifetime of your active account. Once deleted by the user, the data is securely erased or anonymized within a reasonable period, except where legal obligations require longer retention.
- **Payment and Transaction Data:** Billing and transaction records are stored only as long as necessary for financial reporting, taxation, and dispute resolution. Full payment card details are never stored on Pixflame's systems.
- **User-Generated Content:** Photos and other media edited through the App remain stored only on the user's device or in temporary cache files required for processing. When users delete projects or uninstall the App, associated data is automatically removed from our systems.
- **Support Requests and Correspondence:** Communication records with customer support may be stored for a limited period to ensure service quality, usually not exceeding 12 months.

6.2 Marketing and Communication Data

Marketing contact information is retained only until the user unsubscribes or withdraws consent. Once that occurs, the data is permanently deleted from mailing systems or anonymized for internal analytics.

6.3 Technical and Log Data

Technical logs and diagnostic data are kept for short-term operational and security purposes. Typically, such data is retained for no longer than 6–12 months unless required for incident investigation or legal compliance.

6.4 Legal and Regulatory Requirements

Certain Ukrainian and international laws may mandate the retention of accounting and transaction records for up to **seven years**, particularly for tax compliance. In such cases, access to stored information is restricted solely to authorized personnel.

6.5 Secure Deletion and Anonymization

Once the retention period expires, Pixflame employs industry-standard procedures to permanently erase or anonymize data. Secure deletion protocols ensure that removed data cannot be reconstructed, recovered, or linked to any individual. Backups are overwritten on a rolling basis, ensuring continuous data hygiene.

Pixflame's overarching principle is minimal retention — we only keep what is necessary, for as long as necessary, and nothing more.

---

7. International Data Transfers

As a Ukrainian company serving a global user base, **Pixflame** may process and store data in various jurisdictions. While our main infrastructure is hosted within the European Economic Area (EEA) or trusted regions with strong privacy standards, some data may be transferred to countries whose data protection laws differ from those in your jurisdiction.

7.1 Transfer Mechanisms

Your personal data may be processed in:

- **European Union (EU) countries**, ensuring compliance with GDPR-equivalent standards;
- **The United States**, where select cloud infrastructure and analytics providers are based;
- **Other jurisdictions**, strictly limited to where our contracted partners maintain secure technical facilities.

All transfers occur under legally recognized frameworks that ensure adequate protection of personal data.

7.2 Safeguards and Compliance

Pixflame employs the following mechanisms to protect data transferred internationally:

- **Standard Contractual Clauses (SCCs):** Binding contractual provisions approved by the European Commission to ensure equivalent data protection outside the EU;
- **Data Processing Agreements (DPAs):** Signed with all third-party providers to define responsibilities, data handling protocols, and compliance obligations;
- **Technical Safeguards:** Encryption in transit and at rest, multi-factor authentication, and strict access control policies to prevent unauthorized access.

We conduct periodic due-diligence assessments of our service providers to confirm that these safeguards remain effective and compliant with GDPR and Ukrainian law.

7.3 User Consent and Transparency

By using Pixflame, you acknowledge and consent that your data may be transferred and processed outside your country of residence. Regardless of where processing occurs, your data will always receive **the same level of protection** described in this Policy.

Users can contact us at **support@pixflame.co** to request additional information regarding specific transfer mechanisms or safeguards in place.

7.4 Third-Party Providers Abroad

When engaging non-Ukrainian or non-EU service providers, we require that they:

- Use the data only for clearly defined, legitimate purposes;
- Maintain robust technical and organizational measures against unauthorized access;

- Comply with GDPR principles, Ukrainian data protection law, and this Policy.

Pixflame ensures that cross-border data transfers never compromise user privacy or security. Our commitment to transparency and accountability remains unchanged, regardless of geographic boundaries.

---

8. Data Security

Pixflame takes data protection extremely seriously and employs a combination of technical, administrative, and organizational measures to safeguard your personal information from unauthorized access, misuse, loss, or alteration. We continually evaluate our systems and update our security infrastructure to ensure compliance with modern cybersecurity standards.

8.1 Technical Safeguards

- **Encryption in Transit and at Rest:** All sensitive data exchanged between your device and our servers is protected using industry-standard TLS/SSL encryption. Stored data, including backups, is encrypted using strong algorithms such as AES-256.
- **Secure Hosting Environment:** Our cloud infrastructure operates in ISO-certified and GDPR-compliant data centers with restricted physical access, firewalls, and intrusion detection systems.
- **Authentication and Access Controls:** Internal access to data is limited strictly to authorized personnel who require it for operational purposes. Multi-factor authentication and role-based access restrictions are enforced across all administrative systems.
- **Regular Vulnerability Assessments:** Pixflame conducts periodic internal audits, penetration tests, and third-party security reviews to identify and address potential weaknesses before they can be exploited.
- **Data Integrity and Backup Procedures:** Redundant storage systems ensure the availability of data, and regular backups are performed using encrypted channels to prevent data loss.

8.2 Organizational and Procedural Measures

- **Employee Confidentiality:** All employees, contractors, and partners handling user data are bound by written confidentiality agreements and undergo privacy compliance training.
- **Data Handling Policies:** Internal protocols regulate how personal data is accessed, transmitted, and deleted, ensuring minimal exposure risk at every stage.
- **Incident Response Plan:** In the event of a suspected or confirmed data breach, Pixflame initiates a structured incident response protocol that includes:

1. Immediate containment of the threat and forensic investigation;
2. Prompt notification to affected users and authorities, where legally required;
3. Corrective measures to prevent recurrence and strengthen overall resilience.

- **Device and Network Security:** Administrative devices and development environments are protected by updated antivirus software, network firewalls, and secure VPN channels.

8.3 User Responsibilities

While Pixflame implements advanced security measures, users also play a vital role in maintaining data safety. We encourage you to:

- Use a strong, unique password for your account;
- Avoid sharing login credentials with others;
- Keep your device updated and protected against malware;
- Notify us immediately if you suspect unauthorized access to your account.

Pixflame continuously strives to maintain an environment where privacy and security are treated as integral parts of product quality — not optional features.

---

9. Your Rights

Pixflame fully recognizes and supports your rights regarding personal data protection. Depending on your jurisdiction, particularly if you reside in the **European Union** or a country with similar privacy legislation, you may exercise several legal rights concerning the personal information we hold about you.

9.1 Right of Access

You may request confirmation as to whether Pixflame processes your personal data. If so, you have the right to receive a copy of such data along with information about the purposes of processing, categories of data involved, and relevant recipients.

9.2 Right to Rectification

If any personal information we hold about you is inaccurate, incomplete, or outdated, you may request correction or completion at any time. We will respond promptly and update the information within reasonable timeframes.

9.3 Right to Erasure (“Right to be Forgotten”)

You can request deletion of your personal data in cases where it is no longer necessary for the purpose it was collected, when you withdraw consent, or if the data was processed unlawfully. Upon verification, we will securely erase such data from all active systems and backups within a reasonable period.

9.4 Right to Restrict Processing

You may request that we temporarily suspend processing of your personal data if you contest its accuracy, object to its use, or need the data retained solely for legal claims or verification.

9.5 Right to Data Portability

Where technically feasible, you can request a structured, commonly used, machine-readable copy of your personal data, or ask us to transfer it directly to another service provider of your choice.

9.6 Right to Object

You have the right to object at any time to the processing of your personal data for reasons related to your specific situation, including when the processing is based on legitimate interests or involves direct marketing. Once such an objection is made, we will cease processing unless compelling legitimate grounds override your interests or the processing is required by law.

9.7 Right to Withdraw Consent

When processing is based on your consent (for example, for marketing communications or analytics), you may withdraw that consent at any time without affecting the lawfulness of processing carried out prior to withdrawal. You can manage these settings directly in the App or by contacting our support team.

9.8 Rights Related to Automated Decision-Making

If Pixflame uses automated tools, algorithms, or AI-based personalization systems, you have the right not to be subject to decisions made solely by automated processing that significantly affect you. In such cases, human review and explanation are always available upon request.

Pixflame respects all applicable privacy rights equally, regardless of the user's location, and commits to responding to all valid data requests with transparency and care.

---

10. Exercising Your Rights

Pixflame provides simple and transparent methods for users to exercise their privacy rights. We take every request seriously and process it in accordance with applicable data protection laws, including the **GDPR** and Ukrainian privacy legislation.

10.1 How to Submit a Request

To exercise any of your rights described in **Section 9**, please contact us through one of the official communication channels listed in **Section 17 (Contact Information)**. You may send your request by email to **support@pixflame.co** with the subject line *"Privacy Request"*.

For your protection, we may require verification of your identity before taking action — this may include providing a confirmation email or, where legally necessary, a scanned copy of an identification document. We will use this information solely to confirm your identity and will delete it immediately after verification.

10.2 Response Timeframes

Pixflame aims to respond to all valid privacy-related requests **within 30 calendar days**. If a request is complex or involves extensive data retrieval, we may extend this period by up to two additional months, as permitted by law. In such cases, you will receive prior notice explaining the reason for the delay.

10.3 Limitations and Exceptions

Certain legal and operational circumstances may restrict our ability to fulfill specific requests. We may refuse or partially comply with a request when:

- Fulfilling it would compromise another person's privacy or legal rights;
- The information must be retained to comply with a legal or contractual obligation;
- The request is manifestly unfounded, excessive, or repetitive.

In such instances, we will always explain the reason for denial and outline possible alternatives.

10.4 Fees

Pixflame does not charge any fee for handling standard data protection requests. However, where requests are repetitive, disproportionate, or clearly unreasonable, we reserve the right to apply a **reasonable administrative fee** to cover the cost of processing.

10.5 Assistance and Contact

If you believe that your rights have not been adequately respected, you also have the right to file a complaint with your local data protection authority or the **Ukrainian Parliamentary Commissioner for Human Rights**. We encourage users to contact us first so that we can address the issue promptly and amicably.

Pixflame is committed to full transparency, fairness, and cooperation in resolving all privacy-related concerns.

---

11. Cookies and Similar Technologies

Pixflame uses cookies and related technologies to enhance functionality, analyze traffic, and deliver a personalized user experience. These technologies are applied in accordance with GDPR, the **ePrivacy Directive (2002/58/EC)**, and relevant Ukrainian laws.

11.1 What Are Cookies

Cookies are small text files stored on your device when you visit a website or use a web-based application. They help websites remember your actions and preferences (such as login status, language, and region) so you don't have to re-enter them each time you return.

Cookies may also support essential site functionality and provide anonymous analytical data to improve usability and performance.

11.2 Types of Cookies Used by Pixflame

We categorize our cookies into the following groups:

- **Strictly Necessary Cookies:** Required for the proper functioning of our Website, including authentication, session management, and security verification. Without them, some services cannot be provided.
- **Performance and Analytics Cookies:** Collect aggregated data about how visitors use our Website — such as pages viewed, time spent, and technical errors — to improve design and optimize navigation.
- **Functional Cookies:** Allow the Website to remember your preferences, such as chosen language, theme, or previously viewed content.
- **Advertising and Targeting Cookies:** Used by Pixflame and select advertising partners to measure campaign effectiveness and display relevant ads based on anonymized user interactions.
- **Third-Party Cookies:** Placed by analytics or marketing tools such as **Google Analytics** or **Firebase**, always subject to their respective privacy policies.

11.3 Duration and Management

Cookies may be either:

- **Session Cookies**, which expire automatically once you close your browser, or
- **Persistent Cookies**, which remain stored on your device for a defined period or until manually deleted.

You can manage or delete cookies through your browser's settings. Disabling certain cookies may affect functionality, but essential parts of the Website will continue to operate properly.

11.4 Do Not Track and Consent Options

Pixflame respects user preferences related to tracking. You can opt out of analytics or marketing cookies at any time by adjusting cookie settings on our Website. While most modern browsers support "Do Not Track" (DNT) signals, there is currently no industry-wide standard for DNT compliance; therefore, Pixflame does not yet respond to DNT headers. However, we continuously monitor regulatory developments and may introduce this feature once a universal protocol is established.

11.5 Cookies in the App

The Pixflame mobile application itself does not use browser cookies. Instead, it relies on **local storage mechanisms** provided by the operating system (e.g., Android SharedPreferences) for essential functionality, such as remembering user preferences or session data. These records never include personal identifiers or sensitive data and are automatically removed upon uninstalling the App.

Pixflame uses cookies responsibly — only where necessary, with full disclosure and user control over consent preferences.

---

12. Tracking, Analytics, and Third-Party Tools

To continuously enhance performance and deliver the most relevant experience, **Pixflame** relies on a limited set of trusted third-party analytics, advertising, and diagnostic tools. These technologies help us understand how users interact with the App and Website, improve features, and maintain operational stability.

12.1 Purpose of Analytics

Analytics tools allow Pixflame to:

- Measure usage statistics and identify which features are most popular among users;
- Monitor app stability, detect crashes, and optimize performance;
- Analyze aggregated behavior patterns to improve user experience;
- Evaluate the success of marketing campaigns while preserving individual anonymity.

We do not use analytics to track or identify specific individuals. All collected data is aggregated or pseudonymized whenever possible.

12.2 Types of Analytics and Tracking Tools

Pixflame may use the following categories of tools:

- **Google Analytics / Firebase Analytics:** For aggregated usage metrics, session tracking, and crash reporting. These services use anonymized identifiers and operate under Google's Privacy Policy.
- **Google Ads and Conversion Tracking:** To assess the effectiveness of advertising campaigns and optimize ad delivery. This process does not involve direct identification of users.
- **Error and Crash Reporting Services:** Collect limited technical data (device type, OS version, error code) to diagnose bugs and prevent future incidents.
- **Performance Monitoring Tools:** Evaluate resource usage and app responsiveness to ensure stable performance across devices.

Each third-party provider is contractually bound to process data in accordance with applicable laws, solely for the specified purpose, and never for independent marketing or profiling.

12.3 Data Collected by Third-Party Tools

Depending on the specific service, the following types of data may be processed:

- Device model, operating system, browser type, and version;
- IP address (often truncated or anonymized);
- App session duration, screens visited, and event-based interactions;
- Non-identifiable advertising or analytics IDs generated by the operating system (e.g., GAID or Android ID).

No sensitive personal data, such as names, emails, or payment information, is transmitted to analytics platforms.

12.4 Advertising and User Choice

Pixflame may cooperate with advertising networks, such as **Google Ads**, to display non-intrusive ads in the free version of the App.
Users can control ad personalization through their device settings:

- On **Android**, by toggling "Opt out of Ads Personalization" in system settings;
- On **iOS**, via "Limit Ad Tracking" under Privacy > Advertising.

Additionally, users can install browser add-ons such as the Google Analytics Opt-Out Extension to prevent tracking on the Website.

12.5 Transparency and Responsibility

Pixflame discloses all analytics and tracking technologies in this Policy and provides users with the right to opt out where applicable. We never combine analytics data with personally identifiable information or sell aggregated datasets to third parties.

Our use of analytics serves one purpose only — **to understand and improve how Pixflame functions for its users**, not to exploit personal data.

---

13. Third-Party APIs & Integrations

Pixflame enhances its functionality through carefully selected third-party **APIs** and integrations. These integrations enable high-quality editing effects, secure payments, and seamless sharing options — all while maintaining strict privacy and data minimization standards.

13.1 Purpose of Integrations

Pixflame connects to third-party APIs solely to improve or enable specific core features of the App, such as:

- **Photo Processing and AI Enhancement APIs:** Allow application of artistic filters, color corrections, or neural-network–based effects directly within the App.
- **Cloud Storage APIs:** Enable optional backup or synchronization of projects across devices, ensuring that users do not lose their edited content.
- **Payment Provider APIs:** Facilitate subscription purchases via **Google Play Billing** with full encryption and no storage of card data on our servers.
- **Social Media APIs:** Let users share their edited images on platforms like Instagram or Facebook, always at their discretion and with explicit user consent.

Each integration is implemented only to the extent necessary for its intended purpose.

13.2 Data Handling Principles

When interacting with third-party APIs:

- Pixflame limits the data transfer to the minimal scope required for feature functionality;
- All transmissions occur via **encrypted HTTPS/TLS channels**;
- Each partner is vetted for compliance with **GDPR**, Ukrainian privacy law, and relevant platform terms of service;
- Data received from these APIs is never repurposed for unrelated uses or shared with additional third parties.

We maintain internal audit logs documenting when and how data exchanges occur to ensure continuous accountability and traceability.

13.3 Examples of Third-Party Services

To ensure transparency, the following categories of partners may be involved:

- **Google APIs:** for analytics, cloud messaging, and Android integration;
- **Firebase Cloud Services:** for crash reporting and data synchronization;
- **AI Frameworks:** enabling advanced photo editing effects using on-device or cloud-based processing;
- **Payment Gateways:** including Google Play, which handles subscription verification and renewals.

All partners operate under legally binding **Data Processing Agreements (DPAs)**, ensuring confidentiality, integrity, and compliance with international standards.

13.4 User Consent and Awareness

Certain integrations (e.g., sharing content to social media) require explicit user action and permission. The App clearly requests consent before invoking any third-party service that involves data transfer. Users can revoke these permissions at any time through device settings or within the App's interface.

Pixflame maintains full transparency about all third-party collaborations and ensures that integrations serve only one goal — **enhancing creativity and user experience without compromising privacy**.

---

14. App Store & Google Play Compliance

Pixflame is developed, maintained, and distributed in full compliance with the rules and policies of **Google Play** and other relevant mobile app marketplaces. We treat store compliance as an integral part of our responsibility to users, ensuring safety, transparency, and reliability at every stage of the app's lifecycle.

14.1 Policy Compliance and Governance

Pixflame strictly adheres to:

- The **Google Play Developer Program Policies** and **User Data Policy**;
- The **Google Play Payments Policy**, ensuring that all in-app purchases and subscriptions are processed exclusively through Google Play Billing;
- Applicable sections of the **Apple App Store Review Guidelines**, should the app later become available on iOS platforms.

We conduct regular internal reviews and automatic compliance checks before each update to ensure that Pixflame meets all platform requirements, including those related to user data, permissions, and in-app behavior.

14.2 Content Standards

Pixflame does not include or promote any form of prohibited or sensitive content, including:

- Sexually explicit, violent, or hateful materials;
- Misleading, fraudulent, or harmful claims;
- Content that infringes copyright, trademarks, or other intellectual property rights.

All editing features are designed solely for legitimate, creative use — allowing users to stylize and enhance personal photographs while maintaining respect for others' rights and privacy.

14.3 Data and Permission Management

We comply with **Google Play's Data Safety** requirements, providing a clear, accessible disclosure of all data collection and processing practices within both the store listing and this Policy.

Sensitive permissions, such as access to photos, camera, or storage, are requested only when required for the App's core editing functionality. Users are always informed about why a particular permission is needed and may decline or revoke access at any time without losing essential functionality.

14.4 Fair and Transparent Representation

Pixflame's public listings, screenshots, and descriptions accurately reflect the actual features and capabilities of the application. We do not use deceptive wording, fake reviews, or exaggerated claims to attract users.
All marketing materials, whether on Google Play or elsewhere, are verified to match the in-app experience exactly.

14.5 Technical and Security Compliance

Before each release, Pixflame undergoes:

- Security and malware scanning;
- Permission usage validation;
- Manual review of advertising SDKs and libraries to confirm compliance with platform rules.

The app never embeds unauthorized code, hidden trackers, or third-party frameworks that could compromise user data or device security.

14.6 Ongoing Platform Conformity

Pixflame's development team continuously monitors updates to Google Play and Android developer policies. Any required adjustments are implemented proactively to maintain uninterrupted compliance and protect user trust.

By downloading Pixflame, users acknowledge that the application fully adheres to platform policies, ensuring a safe and legitimate user experience backed by transparent operations.

---

15. Children's Privacy

Pixflame is not intended for use by children under the age of **13** (or under **16** in jurisdictions with stricter digital consent requirements, such as the European Union). We consciously design our Services for a general audience of adult and teenage users who wish to edit photos and express creativity responsibly.

15.1 Data Collection from Minors

We do not knowingly collect, store, or process personal information from children. If a user is below the applicable minimum age, they are prohibited from creating an account, making purchases, or using the App's network-dependent features.

If we become aware that we have inadvertently collected personal information from a child without verified parental consent, we will take immediate steps to delete such data from our systems and disable associated accounts.

15.2 Parental Responsibility and Awareness

Parents or legal guardians who believe that their child has interacted with Pixflame in violation of this Policy are encouraged to contact us promptly at **support@pixflame.co**. We will verify the situation and ensure appropriate corrective measures are taken.

Pixflame supports parental control mechanisms available on Android devices (such as **Google Family Link**) and encourages guardians to enable them for additional protection and oversight.

15.3 Educational and Preventive Approach

While Pixflame is not designed for children, we recognize the importance of promoting safe digital behavior. We actively discourage any misuse of the App for harmful or deceptive content creation and reinforce this through our Terms of Service and built-in usage guidelines.

Pixflame's commitment to children's privacy aligns with the principles of the **Children's Online Privacy Protection Act (COPPA)** and the **GDPR provisions for minors**. Our policy is simple: **we do not target, track, or profile minors in any form**.

---

16. Amendments to This Privacy Policy

Pixflame reserves the right to update or modify this Privacy Policy at any time to reflect changes in legal requirements, business practices, or the introduction of new features. Any revisions are made in good faith with the intent to improve clarity, transparency, and user protection.

16.1 Notification of Changes

When significant changes occur, we will inform users through one or more of the following methods:

- Publishing a clear notice on the **Pixflame website**;
- Displaying an in-app notification or pop-up after the update;
- Sending an email to registered users, if applicable.

Each version of the Policy will include a "**Last Updated**" date at the top of the document. Users are encouraged to review this Policy periodically to stay informed about how their data is collected, used, and protected.

16.2 Nature of Amendments

Policy updates may include, but are not limited to:

- Clarifications of existing terms or practices;
- Adjustments in compliance with new data protection regulations (e.g., GDPR or Ukrainian law);
- Inclusion of new service providers or technologies affecting data handling;
- Changes in contact details or company structure.

We ensure that any material updates do not reduce the level of privacy protection guaranteed to our users. If a change materially alters how personal data is processed, we will request renewed consent where required by law.

16.3 User Responsibility

By continuing to use Pixflame after updates take effect, you acknowledge and agree to the revised terms of this Privacy Policy. Users who do not agree with the updated version have the right to discontinue using the Services and request deletion of their data as outlined in **Section 9 (Your Rights)**.

Pixflame maintains archived versions of all previous policies upon request, ensuring full transparency and accountability in the evolution of its privacy practices.

---

17. Contact Information

If you have any questions, concerns, or requests related to this Privacy Policy or your personal data, you can contact us using the following official details:

Legal Entity: FOP Hrymaliuk Pavlo Ivanovych
Tax Identification Number (TIN): 3413810710
Registered Address: 18 Instytutska Street, Apt. 49, Kyiv, 01021, Ukraine
Email: support@pixflame.co
Phone: +380 68 919 6054

Pixflame welcomes inquiries regarding privacy, data security, or compliance.
We aim to respond to all legitimate requests promptly — typically within **30 calendar days** — and to resolve any privacy-related issues in a transparent, respectful, and lawful manner.

If you believe your data rights have been violated or mishandled, you also have the right to file a complaint with the **Ukrainian Parliamentary Commissioner for Human Rights** or the relevant **EU supervisory authority** in your jurisdiction.

Pixflame's dedication to privacy protection is rooted in three core principles:
transparency, accountability, and respect for user autonomy.
We view privacy not as an obligation, but as a continuous commitment to the trust our users place in us.