PRIVACY POLICY

This Privacy Policy (the "Policy") outlines the ways in which Joycee Gifts Ltd (the "Company") collects, processes, and safeguards the personal data of individuals (the "Users") who visit, register, purchase products, or otherwise engage with the website https://joycee.gifts (the "Website").

The Company operates in compliance with Regulation (EU) 2016/679 (GDPR), the UK GDPR, and other relevant data protection laws, including the Data Protection Act 2018 applicable in the United Kingdom.

1. Definitions and Scope

1.1. Personal Data

"Personal Data" encompasses any information that identifies or can be used to identify the User. This may include, but is not limited to name, contact details, IP address, and payment transaction information.

1.2. Scope of Application

1.2.1. This Policy applies to all Personal Data collected through the Website, as well as through related services and communication channels such as email, support chat, and other interactions.

1.2.2. It is applicable to Users located in the EU and the UK and may also extend to Users in other jurisdictions where local laws impose similar data protection requirements (such as the extraterritorial provisions of GDPR/UK GDPR).

1.3. Role of the Company

1.3.1. The Company acts as a "Data Controller" under GDPR/UK GDPR when collecting and utilizing Personal Data from Users.

1.3.2. In specific cases, such as when sharing data with partners for service delivery, the Company may function as a joint controller or data processor, ensuring that all data protection regulations are strictly adhered to.

2. Types of Data Processed

2.1. Data Directly Provided by Users

- Registration Information: Name, surname, email address, and phone number (if required for account creation).
- Payment Information: Payment card details or alternative payment methods. These are typically encrypted and processed by certified payment providers. The Company does not retain full card details unless legally mandated or contractually required.
- Additional User-Provided Data: Any voluntarily shared information, including feedback, support requests, uploaded documents, or screenshots related to technical issues.

2.2. Data Collected Automatically

- Technical and Log Data: IP address, browser type, system language, operating system, timestamps of visits, and referring pages.
- Cookies and Tracking Technologies: Used for user experience optimization, analytics, content personalization, and targeted advertising. For more details, refer to the Cookie Policy.

2.3. Data from Third-Party Sources

- Partner Services: If Users opt for OAuth-based login or social media sign-ins, relevant account details (e.g., email, profile name) may be transferred to the Company.
- Financial and Payment Providers: When making transactions, the Company may receive confirmation or status updates from payment providers.
- KYC/AML Compliance Providers: To comply with Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations, the Company may obtain identity verification data and risk assessments from external compliance partners.

For identity verification purposes, the Company may engage specialized third-party service providers (e.g., SumSub) to process verification documents under strict contractual safeguards.

This Policy ensures that the Company remains committed to protecting the User's Personal Data in accordance with global privacy standards.

3. Purposes and Legal Bases of Processing

Note: References to Art. 6(1) GDPR also apply to UK GDPR, unless stated otherwise.

3.1. Contract Performance and Service Provision (Art. 6(1)(b) GDPR/UK GDPR)

- Facilitating account registration and login, providing access to a personal account, processing orders, and delivering digital codes or granting access to purchased content.
- Communicating with Users regarding transactions, service updates, and order status notifications.

3.2. Legitimate Interests (Art. 6(1)(f) GDPR/UK GDPR)

- Enhancing Website functionality, collecting analytics and statistical data, preventing fraud, and ensuring overall system security (including detection and investigation of security incidents).
- Conducting marketing activities within reasonable limits, including personalized content recommendations based on prior interactions.
- Carrying out AML (Anti-Money Laundering) and CTF (Counter-Terrorism Financing) procedures, if required to assess profile risks or transaction integrity.

Where permitted by law, the Company may use profiling to assess transaction patterns, detect potential fraud, or tailor its communications to User interests.

3.3. Consent (Art. 6(1)(a) GDPR/UK GDPR)

- Sending marketing and promotional emails, where separate opt-in consent is legally required.
- Using non-essential cookies and tracking technologies, subject to User consent as required by local regulations (e.g., PECR in the UK, ePrivacy Directive in the EU).

3.4. Compliance with Legal Obligations (Art. 6(1)(c) GDPR/UK GDPR)

- Retaining transaction records for taxation, accounting, and financial reporting in accordance with legal requirements.
- Fulfilling AML/CTF compliance obligations, such as monitoring transactions, conducting PEP (Politically Exposed Persons) and sanctions list screenings, and cooperating with regulatory authorities.

4. Data Retention Periods

4.1. General Principles

4.1.1. Personal Data is retained only for as long as necessary to fulfill the purposes outlined in this Policy or as required by law.

4.1.2. Retention periods vary based on Personal Data category (e.g., tax-related documentation must be kept for a minimum of five (5) years, or longer as required under UK law).

4.2. Criteria for Determining Retention Periods

- Account activity status (Personal Data data is retained while the account remains active).
- Legal obligations concerning taxation, accounting, and financial reporting.
- Marketing consent duration (Personal Data is retained for marketing purposes until consent is withdrawn by the User).
- KYC-related documents are retained in accordance with AML legislation for a minimum period of five (5) years from the date of verification, or longer where required by applicable law.

4.3. Data Deletion or Anonymization

4.3.1. Once retention periods expire, the Company ensures secure deletion or anonymization of Personal Data.

4.3.2. If a User requests account deletion, and no legal basis exists for continued Personal Data retention, the Personal Data will be erased within a reasonable timeframe (see “User Rights” section for more details).

5. Data Sharing and Disclosure

5.1. Internal Data Access

Personal Data is accessible only to Company employees whose roles require it, following the “need-to-know” principle to maintain Personal Data confidentiality.

5.2. Sharing with Third Parties

The Company may share Personal Data with:

- Payment Service Providers – to facilitate and process transactions securely.
- Analytics Services (e.g., Google Analytics) – to gather statistical insights (see Cookie Policy for more details).
- IT Contractors and Hosting Providers – for server hosting, database management, and overall IT infrastructure support.
- KYC/AML Compliance Services – to conduct identity verification, anti-money laundering (AML), and counter-terrorism financing (CTF) screenings.
- Regulatory and Government Authorities – when legally required, such as responding to law enforcement requests under EU or UK laws.

5.3. International Data Transfers

If Personal Data is transferred outside the EU/EEA or the UK, the Company ensures compliance with GDPR/UK GDPR standards, implementing safeguards such as:

- Standard Contractual Clauses (SCCs) for international data transfers.
- Assessments of the recipient country's data protection levels to determine adequacy.

6. Data Protection and Security Measures

6.1. Technical and Organizational Safeguards

To protect Personal Data from unauthorized access, loss, or misuse, the Company employs:

- Encrypted communication protocols (HTTPS/TLS) to secure Personal Data in transit.
- Strict access control mechanisms, ensuring role-based permissions for databases.
- Continuous security monitoring to identify vulnerabilities and regular system backups.
- Internal policies and staff training, including Non-Disclosure Agreements (NDAs) and access limitations.

6.2. Data Breach Notification

6.2.1. In the event of a Personal Data breach, the Company will promptly notify the appropriate supervisory authorities (e.g., ICO in the UK, local Data Protection Authorities in the EU) in compliance with Articles 33 and 34 of GDPR/UK GDPR.

6.2.2. If required, affected Users will also be informed about the breach and any recommended protective actions.

7. User Rights

Under the GDPR and UK GDPR, the User has the following rights in relation to their Personal Data:

1. **Right of Access** (Art. 15) – The User has the right to request a copy of their Personal Data held by the Company, along with information regarding its processing.
2. **Right to Rectification** (Art. 16) – The User may request the correction of any inaccurate or incomplete Personal Data.
3. **Right to Erasure ("Right to be Forgotten")** (Art. 17) – The User may request the deletion of their Personal Data where:
   - the data is no longer necessary for the purpose for which it was collected;
   - the User withdraws consent, where consent was the legal basis for processing;
   - there are no overriding legal grounds for the retention of the data.
4. **Right to Restrict Processing** (Art. 18) – The User may request the restriction of processing of their Personal Data under certain circumstances, such as where the accuracy of the data is contested or the processing is unlawful.
5. **Right to Data Portability** (Art. 20) – The User may obtain a structured, commonly used, and machine-readable format of their Personal Data and, where technically feasible, request the transmission of such data to another data controller, provided that the processing is based on consent or contract.
6. **Right to Object** (Art. 21) – The User has the right to object to the processing of their Personal Data, including for direct marketing purposes.
7. **Right to Withdraw Consent** (Art. 7(3)) – Where processing is based on the User's consent, the User has the right to withdraw such consent at any time without affecting the lawfulness of processing carried out prior to withdrawal.

To exercise any of these rights, the User may contact the Company using the contact details provided below.

For verification and security purposes, the Company may request proof of identity before acting on any such request.

8. Cookies and Similar Technologies

8.1. The Company employs cookies and similar tracking technologies to enhance the User's experience, facilitate personalization, and conduct analytics. Detailed information on the use and management of cookies is provided in the Company's Cookie Policy, which forms an integral part of this Privacy Policy.

8.2. Where certain categories of cookies require the User's consent, a Cookie Consent Banner or pop-up (opt-in mechanism) may be presented upon the User's initial visit to the Website or at periodic intervals thereafter.

8.3. In the United Kingdom, the use of non-essential cookies is governed by the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR). In the European Union, such use falls under the ePrivacy Directive or applicable national legislation implementing it.

9. Marketing and Communications

9.1. Email and Push Notifications

9.1.1. If the User has provided explicit consent, the Company may send informational and promotional messages. Every such communication includes an unsubscribe option that allows the User to withdraw from further marketing messages at any time.

9.1.2. Opting out of marketing emails does not affect the ability to receive important service-related communications, such as order confirmations, updates on purchases, or notifications about critical changes to the Website.

9.2. Third-Party Advertising

9.2.1. The Website may display personalized advertisements tailored to User interests and past interactions. These may involve third-party cookies or similar tracking technologies.

9.2.2. Users can manage or disable such targeted advertising by adjusting their browser settings or utilizing available opt-out mechanisms.

10. Children and Minimum Age

10.1. The Company does not knowingly collect, process, or store Personal Data from individuals under the age of sixteen (16), or any higher minimum age defined by applicable local laws.

10.2. If the Company becomes aware that a child's Personal Data has been collected without verifiable consent from a parent or legal guardian, the Company will take immediate steps to remove such Personal Data from its systems.

10.3. If a parent or legal guardian believes that the User, who is a child, has submitted Personal Data to the Company, they are encouraged to contact the Company without delay using the contact details provided below.

11. Compliance with AML/CTF Regulations

11.1. In cases where applicable law requires Know Your Customer (KYC) and Anti-Money Laundering (AML) checks, the Company may request Users to submit additional verification documents, including but not limited to:

- Passport or national ID
- Proof of address (e.g., utility bill, bank statement)
- Other documents relevant for compliance purposes

11.2. All such Personal Data is processed in strict accordance with this Privacy Policy and the AML/CTF Policy. The collection and storage of identity documents occur only

when legally mandated and based on a valid legal ground (e.g., necessity for compliance with regulatory obligations).

12. Changes to This Policy

12.1. Policy Updates

The Company reserves the right to modify or update this Policy periodically. Updates may occur in particular, but not exclusively, in the following circumstances:

- the implementation of new technologies or security measures;
- compliance with amendments to applicable data protection laws;
- the expansion of the Website's features or services.

The most recent version of this Policy will always be made available on the Website.

12.2. User Notifications

In the event of material changes to this Policy, the Company may notify the User through one or more of the following methods:

- a clearly visible notice published on the Website;
- direct communication (e.g., via email), where required by law and where the Company holds the User's contact information.

13. Contact Information

For any inquiries related to this Policy, the User's Personal Data, or the User's privacy rights, the Company may be contacted using the details provided below:

- Company Name: Joycee Gifts Ltd
- Postal address: 311 Shoreham St, Highfield, Sheffield S2 4FA, United Kingdom
- Website: https://joycee.gifts
- Privacy-related inquiries: privacy@joycee.gifts
- Compliance matters: compliance@joycee.gifts

14. Final Provisions

14.1. This Privacy Policy forms an integral part of the broader legal framework governing the use of the Website. This includes, but is not limited to, the following documents:

- Terms & Conditions
- Cookie Policy
- Refund Policy
- KYC Policy
- AML/CTF Policy

14.2. By accessing or using the Website and/or by submitting Personal Data to the Company, the User acknowledges that they have read, understood, and agreed to the terms of this Privacy Policy.

14.3. If any provision of this Privacy Policy is held to be invalid, unlawful, or unenforceable, such provision shall be deemed severable and shall not affect the validity and enforceability of the remaining provisions, which shall remain in full force and effect.

Last Updated: 23.10.2025