EasyPeasy RoPA

Record of Processing Activities (RoPA)

1. Name and Contact Details of the Controller

- **Controller Name:** EasyPeasy
- **Address:** X+Why, 20-30 Whitechapel Road, London, E1 1EW
- **Data Protection Officer:** Jen Lexmond (EasyPeasy DPO)
- **Contact Information:** DPO EasyPeasy

---

2. Purposes of Processing

EasyPeasy processes personal data for the following purposes:

- Account creation and user authentication (including OAuth integration).
- Delivery of personalised and localised app content based on user interactions and demographics.
- Analysis of app usage data to improve user experience and app performance.
- Email newsletter subscription management.
- Provision of customer support and handling user queries.
- Marketing analysis and management, including user segmentation for targeted communication.
- Compliance with legal obligations, including data protection and security standards.

3. Description of Data Processed and Data Subjects

- **Categories of Data:**
  - **Identity Data:** Full name, username.
  - **Contact Data:** Email address, postcode.
  - **Technical Data:** IP address, login data, browser type and version, time zone setting.
  - **Profile Data:** User preferences, interests, and feedback.
  - **Usage Data:** Information on how users interact with the website, app, and services.
  - **Special Category Data:** Ethnicity (optional in surveys), children's first names and dates of birth.
- **Data Subjects:**
  - Registered users of the EasyPeasy app.
  - Trainees in training programs.
  - Clients who have engaged EasyPeasy services.
  - Staff employed by EasyPeasy.
  - Individuals who submit support requests.

---

4. Description of Data Processed and Legal Bases

The following tables detail the specific data points collected and processed by EasyPeasy across different user groups, along with the corresponding legal bases for processing under Articles 6 and 9 of the UK GDPR.

Users

Data Point	Purpose of Collection	Legal Basis (Article 6)	Legal Basis (Article 9)
Full Name	App usage and personalisation	Contractual Necessity (Article 6(1)(b))	N/A
Email	App usage and personalisation	Legitimate Interests (Article 6(1)(f))	N/A
Postcode	App usage and personalisation	Contractual Necessity (Article 6(1)(b))	N/A
Password	Account security and authentication	Contractual Necessity (Article 6(1)(b))	N/A
Username	App usage and personalisation	Legitimate Interests (Article 6(1)(f))	N/A
Child's First Name	Personalised content delivery	Explicit Consent (Article 6(1)(a))	Explicit Consent (Article 9(2)(a))

Child's Date of Birth	Personalised content delivery	Explicit Consent (Article 6(1)(a))	Explicit Consent (Article 9(2)(a))
Profile image	App usage and personalisation	Consent (Article 7(1)(a))	N/A
Bio	App usage and personalisation	Consent (Article 7(1)(a))	N/A
Ethnicity (optional survey)	Monitoring and ensuring equal opportunities	Explicit Consent (Article 6(1)(a))	Explicit Consent (Article 9(2)(a))
Gender (optional survey)	Monitoring and ensuring equal opportunities	Explicit Consent (Article 6(1)(a))	Explicit Consent (Article 9(2)(a))
Device Information (IP, Browser)	Security, app usage analytics	Legitimate Interests (Article 6(1)(f))	N/A
Content Interaction Data	App usage analytics and personalisation	Legitimate Interests (Article 6(1)(f))	N/A

Payment Information (Stripe)	In-app purchases, subscription management	Contractual Necessity (Article 6(1)(b))	N/A
Contact number	Invite to the platform	Legitimate Interests (Article 6(1)(f))	N/A
Email	Invite to the platform	Legitimate Interests (Article 6(1)(f))	N/A
First name	Invite to the platform	Legitimate Interests (Article 6(1)(f))	N/A
Last Name	Invite to the platform	Legitimate Interests (Article 6(1)(f))	N/A

Trainees

Data Point	Purpose of Collection	Legal Basis (Article 6)	Legal Basis (Article 9)
Full Name	Training administration	Contractual Necessity (Article 6(1)(b))	N/A

Email	Training administration	Contractual Necessity (Article 6(1)(b))	N/A
Job Title	Record of attendance and certification	Contractual Necessity (Article 6(1)(b))	N/A
Local Authority	Record of attendance and certification	Contractual Necessity (Article 6(1)(b))	N/A
Org name	Record of attendance and certification	Contractual Necessity (Article 6(1)(b))	N/A
Training Participation	Record of attendance and certification	Contractual Necessity (Article 6(1)(b))	N/A
Feedback Data	Improving training programs	Legitimate Interests (Article 6(1)(f))	N/A

Clients

Data Point	Purpose of Collection	Legal Basis (Article 6)	Legal Basis (Article 9)

Client First Name	Client relationship management	Legitimate Interests (Article 6(1)(f))	N/A
Client Last Name	Client relationship management	Legitimate Interests (Article 6(1)(f))	N/A
Client Email	Client relationship management	Legitimate Interests (Article 6(1)(f))	N/A
Contact Information	Client communication	Legitimate Interests (Article 6(1)(f))	N/A
Job Title	Client relationship management	Legitimate Interests (Article 6(1)(f))	N/A
Local Authority	Client relationship management	Legitimate Interests (Article 6(1)(f))	N/A
Org name	Client relationship management	Legitimate Interests (Article 6(1)(f))	N/A

Billing Information	Invoice processing and payment tracking	Contractual Necessity (Article 6(1)(b))	N/A

Staff

Data Point	Purpose of Collection	Legal Basis (Article 6)	Legal Basis (Article 9)
Staff First Name	Employment management	Contractual Necessity (Article 6(1)(b))	N/A
Staff Surname	Employment management	Contractual Necessity (Article 6(1)(b))	N/A
Email	Employment management	Contractual Necessity (Article 6(1)(b))	N/A
Role	Employment management	Contractual Necessity (Article 6(1)(b))	N/A

National Insurance number	Employment management	Contractual Necessity (Article 6(1)(b))	N/A
Date of Birth	Employment management	Contractual Necessity (Article 6(1)(b))	N/A
Phone number	Employment and legal compliance	Legal Obligation (Article 6(1)(c))	N/A
Payroll Information	Salary processing and financial records	Contractual Necessity (Article 6(1)(b))	N/A
Next of Kin	Employment management	Contractual Necessity (Article 6(1)(b))	N/A
Passport image	Employment management	Contractual Necessity (Article 6(1)(b))	N/A
Performance Data	Employee performance evaluation	Legitimate Interests (Article 6(1)(f))	N/A

Tax code	Employment management	Contractual Necessity (Article 6(1)(b))	N/A
P45	Employment management	Contractual Necessity (Article 6(1)(b))	N/A
Bank Details	Employment management	Contractual Necessity (Article 6(1)(b))	N/A
Health Data	Managing employee well-being and sick leave	Legal Obligation (Article 6(1)(c))	Explicit Consent (Article 9(2)(a))
Right to work in the UK	Employment management	Contractual Necessity (Article 6(1)(b))	N/A

Support Requests

Data Point	Purpose of Collection	Legal Basis (Article 6)	Legal Basis (Article 9)

First Name	Support request handling	Legitimate Interests (Article 6(1)(f))	N/A
Last Name	Support request handling	Legitimate Interests (Article 6(1)(f))	N/A
Personal Email	Support request handling	Legitimate Interests (Article 6(1)(f))	N/A
Description of Request	Support request resolution	Contractual Necessity (Article 6(1)(b))	N/A
Technical Details (e.g., screenshots)	Debugging and resolving technical issues	Legitimate Interests (Article 6(1)(f))	N/A

5. Recipients of Personal Data

- **Internal Recipients:**
  - Product team, Marketing team, Customer Support.
- **External Recipients (Third-Party Organizations):**
  - **Analytics and Monitoring:**
    - Google Analytics
    - Firebase Analytics

- - - Smartlook
    - AppsFlyer
    - Sentry
    - Google Tag Manager
    - LaunchDarkly
  - **CRM and Communication:**
    - HubSpot
    - OneSignal
    - Slack
    - MS Teams
    - Zoom
    - AirShip
    - SurveyMonkey
    - Metis
  - **Payments and Financial Services:**
    - Stripe
    - Wise
    - Sage
    - Xero
    - HSBC
  - **Cloud and Data Hosting:**
    - Amazon Web Services (AWS)
    - Google Workspace
    - Postgres Database (within AWS)
    - Cloudinary (for media data transfer)
  - **User Authentication and Social Login:**
    - Google OAuth
    - Apple Sign-In
  - **Marketing and Ad Services:**

- Google Ads
- Meta (Facebook)
- Recombee
- Impact Dashboard
- Apps Radar
- Charlie HR
- Upwork
- **Customer Support and Feedback:**
  - HubSpot
  - MS Office Mail
  - Appsflyer
  - Smartlook
  - Recombee
  - Google Workspace
- **Others:**
  - Quicksight
  - Wise
  - SeedLegals
  - Iubenda
  - TestFlight
  - Play Store beta testing

Each of these third-party organisations processes personal data on behalf of EasyPeasy and is bound by data processing agreements that include appropriate safeguards, such as Standard Contractual Clauses (SCCs), to ensure GDPR compliance.

---

6. Details of Transfers to Third Countries

EasyPeasy shares personal data with a range of third-party organisations to fulfil various business functions, including analytics, communication, payment processing, and customer support. Below is a detailed list of these organisations, the countries where data processing occurs, and the specific safeguards that ensure compliance with the UK GDPR:

- **Sage Pay (UK)**
  - **Purpose:** Payroll and employment requirements.
  - **Data Categories:** Employee records, payroll information.
  - **Safeguards:** Encryption, access control, regular audits.
  - **Data Processing Location:** United Kingdom.
- **GMBC (UK)**
  - **Purpose:** Employment requirements.
  - **Data Categories:** Employee records, payroll information.
  - **Safeguards:** Access control, regular audits.
  - **Data Processing Location:** United Kingdom.
- **SurveyMonkey (USA)**
  - **Purpose:** Collecting feedback.
  - **Data Categories:** Email addresses.
  - **Safeguards:** Encryption, access control.
  - **Data Processing Location:** United States.
  - **Transfer Mechanism:** Standard Contractual Clauses (SCCs).
- **Slack (USA)**
  - **Purpose:** Team communication and collaboration.
  - **Data Categories:** Name, email address, work address, telephone number.
  - **Safeguards:** Access control, encryption.
  - **Data Processing Location:** United States.
  - **Transfer Mechanism:** Standard Contractual Clauses (SCCs).
- **Trello (USA)**
  - **Purpose:** Project management and collaboration.
  - **Data Categories:** Name, email address, work address, telephone number.

- ○ **Safeguards:** Access control, encryption.

- ○ **Data Processing Location:** United States.

- ○ **Transfer Mechanism:** Standard Contractual Clauses (SCCs).

- **HubSpot (USA and EU)**

  - ○ **Purpose:** CRM and email management.

  - ○ **Data Categories:** Contact information, interaction history.

  - ○ **Safeguards:** Encryption, regular audits.

  - ○ **Data Processing Locations:** United States, European Union.

  - ○ **Transfer Mechanism:** Standard Contractual Clauses (SCCs) for data transferred outside the EU.

- **Stripe (USA)**

  - ○ **Purpose:** Payment processing.

  - ○ **Data Categories:** Payment information, transaction history.

  - ○ **Safeguards:** Encryption, PCI DSS compliance.

  - ○ **Data Processing Location:** United States.

  - ○ **Transfer Mechanism:** Standard Contractual Clauses (SCCs).

- **Amazon Web Services (AWS) (Europe)**

  - ○ **Purpose:** Cloud data storage and hosting.

  - ○ **Data Categories:** All categories of personal data.

  - ○ **Safeguards:** Encryption at rest and in transit, role-based access control (RBAC).

  - ○ **Data Processing Locations:** United Kingdom, European Union, United States, and other AWS regions.

  - ○ **Transfer Mechanism:** Standard Contractual Clauses (SCCs) for data transferred outside the EU.

- **Google Workspace (Global)**

  - ○ **Purpose:** Email and document management.

  - ○ **Data Categories:** Contact information, document content.

  - ○ **Safeguards:** Encryption, access control, regular audits.

  - ○ **Data Processing Locations:** United States, European Union.

- ○ **Transfer Mechanism:** Standard Contractual Clauses (SCCs).
- ● **Recombee (EU)**
  - ○ **Purpose:** Recommendation engine.
  - ○ **Data Categories:** User interaction data.
  - ○ **Safeguards:** Pseudonymization, encryption.
  - ○ **Data Processing Location:** European Union.
- ● **Others (Various Locations)**
  - ○ **Additional third-party processors** such as Upwork, Zoom, Xero, etc., handle specific tasks ranging from project management to financial processing, each with appropriate data protection measures in place. Detailed descriptions and safeguards are outlined in the data sharing register.

In all cases where personal data is transferred outside the UK or EU, EasyPeasy ensures compliance with GDPR by implementing Standard Contractual Clauses (SCCs) and conducting regular security and compliance checks with these third-party processors.

---

7. Retention Periods

- ● **Identity and Contact Data**:
  - ○ Retained until the account is deleted, the child reaches 18 years of age, or we are informed that the user is no longer a practitioner. If no date of birth (D.O.B) is provided on the account, the data is retained until the account has been registered for 8 years and 1 day.
  - ○ Uncompleted Registration (Email and Password): If a user does not complete registration, their email and password will be retained for 60 days after initiating the registration process. After this period, the email and password are permanently deleted.
  - ○ Password, Username, Bio, and Profile Image: Retained until the account is deleted, the child reaches 8 years and 1 day of age, or we are informed that the

user is no longer a practitioner. If no date of birth is provided, this data is retained until the account has been registered for 8 years and 1 day.

  ○ More details are outlined in the [PII legal processing](#) and [3rd party data sharing registers](#).

- **Special Category Data**: [Retained only as long as necessary](#) for survey aggregation and anonymisation.

- **Technical and Usage Data**: Retention periods are specified in the [DPIA](#) and are aligned with legal requirements and applicable limitation periods.

---

8. Technical and Security Measures

As outlined in the **[Data Flow Security Measures](#)** document:

- **Data Collection:** Secure forms, OAuth for authentication, and encrypted connections.

- **Data Transmission:** TLS/SSL protocols, VPNs, and secure remote access.

- **Data Storage:** Encryption at rest, firewalls, and restricted access with MFA.

- **Data Access:** Role-based access control (RBAC), audit logs, and user training.

- **Data Retention and Deletion:** Secure deletion methods, regular audits, and compliance with data destruction policies.