Schedule 4 (Data processing information)

1. Categories of data subject

The Customer Personal Data processed under this Agreement may relate to the following categories of data subjects:

(a) **Customer Personnel:** The Customer's employees, officers, volunteers, contractors, and authorized users who create and manage quizzes and other outputs using the Hosted Services.

(b) **Quiz Participants:** Individuals who complete quizzes created by the Customer, including the Customer's existing supporters, donors, volunteers, and prospective supporters.

(c) **Contact Records:** Individuals whose contact information is synchronized with the Hosted Services through Third Party Services integrations (such as Engaging Networks).

2. Types of Personal Data

The Customer Personal Data processed under this Agreement may include:

(a) **Identity and Contact Data:**
- Names (first name, last name)
- Email addresses
- Phone numbers (if collected by Customer)
- Job titles or organizational roles (for Customer Personnel)
- Language spoken

(b) **Account and Authentication Data:**
- Account credentials (usernames, hashed passwords)
- User roles and permissions
- Account preferences and settings

(c) **Quiz Response Data:**
- Quiz answers and submissions
- Quiz completion times and dates
- Quiz scores and results

(d) **Location Data:**
- IP addresses
- Geographic location data (country, region, city) derived from IP addresses or voluntarily provided by

quiz participants for local campaign information features
- Postcode or ZIP code (if collected by Customer)

(e) **Technical and Usage Data:**
- Browser type and version
- Device information (type, operating system)
- Cookies and similar tracking technologies
- Usage logs and analytics (pages viewed, features used, time spent)
- Date and time stamps of activities

(f) **Integration Data:**
- Data synchronized from or to Third Party Services (Engaging Networks, Mailchimp)
- Tags, segments, or custom fields from integrated platforms

(g) **Communications and Support Data:**
- Support ticket content and correspondence
- Customer Personnel names and email addresses submitting support requests
- Account identifiers and subscription details provided in support context
- Screenshots, log files, or data samples shared for troubleshooting purposes
- Support ticket metadata (submission time, status, priority, resolution)
- Customer satisfaction ratings and feedback

(h) **Special Categories of Personal Data:**

The Provider does not require the Customer to process special category personal data through the Hosted Services. However, the Customer may choose to collect special categories through quiz responses, including:

- Political opinions (e.g., policy preferences, party affiliation)
- Religious or philosophical beliefs
- Health data
- Trade union membership
- Racial or ethnic origin

If the Customer processes special category personal data:

(i) The Customer must have appropriate lawful bases under Article 9 GDPR (explicit consent, substantial public interest, etc.)

(ii) The Customer must implement appropriate additional safeguards

(iii) The Customer must document the legal basis in its data protection records

(iv) The Provider will process such data under the same robust technical and organizational security measures as other Personal Data (as detailed in Section 4), which are designed to be appropriate for special category data requiring enhanced protection

3. Purposes of processing

Customer Personal Data is processed for the following purposes:

(a) Service Provision:
- To provide the quiz creation, hosting, and management functionality
- To enable Customer Personnel to create, edit, publish, and manage quizzes
- To deliver quizzes to quiz participants and record their responses
- To generate quiz results, analytics, and reports

(b) Integration Services:
- To transmit Customer Personal Data to Third Party Services (such as Engaging Networks) as configured and instructed by the Customer
- To facilitate data synchronization between the Hosted Services and Third Party Services on the Customer's behalf
- To enable the Customer to use quiz data in their existing CRM, email marketing, and advocacy platforms

(c) Local Campaign Features:
- To display location-relevant information to quiz participants based on their geographic location

- To enable advocacy campaigns targeting specific regions or constituencies

(d) Account Management:
- To create and maintain Customer accounts
- To authenticate and authorize users
- To manage subscriptions and billing

(e) Service Support and Improvement:
- To provide technical support and customer service via email, live chat, and support portal
- To track, manage, and resolve support tickets and inquiries
- To maintain support communication history for continuity and quality assurance
- To troubleshoot errors and resolve technical issues
- To maintain, improve, and develop the Hosted Services
- To conduct aggregated analytics and create anonymized, non-reversible benchmarks (where Personal Data has been irreversibly de-identified such that individuals cannot be re-identified, meaning the data is no longer Personal Data under GDPR)
- To analyze support patterns and improve service quality
- To send service-related notifications and updates

(f) Security and Compliance:
- To detect, prevent, and respond to security incidents
- To prevent fraud and abuse
- To comply with legal and regulatory obligations

4. Security measures for Personal Data

The Provider implements the following technical and organizational security measures:

4.1 Technical Measures

(a) Encryption:
- All data in transit is encrypted using TLS 1.2 or higher (HTTPS)
- All data at rest is encrypted using AES-256 encryption
- Database encryption is provided by Supabase and Redis with encryption keys managed securely

(b) Access Controls:

- Role-based access control (RBAC) for Customer accounts
- Multi-factor authentication (MFA) available for Customer accounts
- Principle of least privilege applied to all system access
- Authentication tokens with automatic expiration after 8 hours (or after 4 hours of inactivity)
- Regular review and revocation of unnecessary access rights

(c) Network Security:

- Firewalls protecting database and application infrastructure
- DDoS protection provided by Vercel Firewall
- Network segmentation between production and development environments
- Regular security patching and updates

(d) Data Backup and Recovery:

- Automated daily backups retained for 7 days
- Backups encrypted at rest (AES-256)
- Primary backup location: Frankfurt, Germany
- Quarterly backup restoration testing
- Disaster recovery plan with 24-hour recovery time objective

(e) Monitoring and Logging:

- Security event logging and monitoring
- Automated alerts for suspicious activities
- Log retention for 30 days
- Regular log review and analysis

4.2 Organizational Measures

(a) Personnel Security:

- Confidentiality agreements for all personnel
- Regular security awareness training
- Clear data protection roles and responsibilities

(b) Access Management:

- Documented procedures for granting and revoking access
- Regular access reviews (at least annually)

- Immediate access revocation upon personnel departure
- Secure credential management

(c) Incident Response:
- Written security incident response plan
- Designated security incident response team
- 24-hour breach notification process (Clause 19.12)
- Incident documentation and post-incident review

(d) CDN Security (Cloudflare):
- Cloudflare CDN serves static assets (HTML, CSS, JavaScript, images) only
- No Personal Data is transmitted through or stored on Cloudflare
- DDoS protection at CDN level for availability
- TLS encryption for all static asset delivery
- Automatic HTTPS upgrades
- Security headers (HSTS, CSP, X-Frame-Options)
- Certificate management and automatic renewal

(e) Vendor Management:
- Due diligence on sub-processors (Supabase, Redis, Vercel, Sentry, Stripe)
- Contractual data protection obligations for sub-processors
- Regular review of sub-processor security practices

(f) Security Testing and Audits:
- Regular vulnerability assessments
- Annual security reviews of infrastructure
- Penetration testing (at least annually or after significant changes)
- Review and update of security policies and procedures

(g) Data Minimization and Retention:
- Collection limited to data necessary for specified purposes
- Retention periods defined and documented
- Secure deletion procedures using industry-standard methods
- Regular review and deletion of unnecessary data

(h) Infrastructure Security (Vercel)

- Vercel hosts the application, API,dashboard, and serves dynamic content from Frankfurt, Germany (EU)
- All Personal Data processed through Vercel infrastructure is encrypted in transit (TLS 1.2+) and at rest
- Automatic HTTPS enforcement for all endpoints
- DDoS protection and Web Application Firewall (WAF) capabilities
- SOC 2 Type II certified infrastructure

5. Sub-processors of Personal Data

The Provider engages the following sub-processors to process Customer Personal Data:

Sub-processor	**Service Provided**	**Location of Processing**	**Data Processed**
Supabase Inc.	Database hosting, authentication, file storage	Frankfurt, Germany (EU)	All Customer Personal Data
Vercel Inc.	Application hosting, API hosting, CDN hosting, data processing	Frankfurt, Germany (EU)	All Customer Personal Data processed through the dashboard and API (including quiz submissions)
Redis	Database and caching services	Frankfurt, Germany (EU)	Quizzes content and settings, Quiz Participants data (quiz submissions)
Stripe, Inc.	Payment processing	Ireland (EU) and USA	Customer name, email, payment card details (tokenized), billing address, transaction data
Quality Unit, LLC (LiveAgent)	Customer support ticketing and helpdesk	Slovakia (EU)	Customer Personnel contact details (name, email), support request

			content, account information, conversation history, attachments (may include screenshots containing Customer Data)
Sentry (Functional Software, Inc.)	Error logging	Frankfurt, Germany (EU)	Error logs (may include personal data, including IP address, email address, and any other personal information collected by users in the dashboard and in forms on quizzes)
Fly.io, Inc.	Application hosting for Third Party Service integrations (data transmission to Engaging Networks)	Frankfurt, Germany (EU)	Quiz Participant data transmitted to Third Party Services, which may include names, email addresses, phone numbers, postcodes, quiz responses, scores, and custom fields as configured by the Customer
Amazon Web Services, Inc. (AWS)	Database backup storage	Frankfurt, Germany (EU)	Encrypted database backups containing Quizzes content and settings, Quiz Participants data (quiz submissions)

5.1 Sub-processor Locations and Safeguards

(a) Primary Processing (EU):

- Supabase: All database storage and primary data processing occurs in Frankfurt, Germany (EU data center)
- Vercel: All application hosting, API hosting, and data processing occurs in Frankfurt, Germany (EU data center)

- LiveAgent: All support ticket processing occurs in Slovakia (EU)
- Sentry: Error logging occurs in Frankfurt, Germany (EU data center)
- Stripe: Payment processing primarily in Ireland (EU), with some processing in USA
- Fly.io: Integration services and data transmission processing occurs in Frankfurt, Germany (EU data center)
- Redis: Database and caching services occur in Frankfurt, Germany (EU data center)
- AWS: Database backup storage occurs in Frankfurt, Germany (EU data center)

(b) Cloudflare Static Assets:

Cloudflare hosts static files (HTML, CSS, JavaScript, images) on its global CDN for performance optimization

- Static files do not contain Personal Dat
- No Personal Data is processed, stored, or transmitted through Cloudflare's services
- Cloudflare serves only public, non-personal content

(c) All Personal Data Processing Occurs in EU: All Customer Personal Data is processed and stored exclusively within the European Union (Frankfurt, Germany; Slovakia; and other EU locations), with the exception of payment processing by Stripe (Ireland and USA).

(d) Transfers Outside EEA

The only transfer of Personal Data outside the EEA is to Stripe (USA) for payment processing. This transfer is protected by:

- Standard Contractual Clauses (Decision 2021/914)
- Transfer Impact Assessment
- Supplementary technical measures (encryption, access controls, tokenization of payment card data)

(e) Adequacy Decisions:

- Ireland benefits from EU adequacy decision (within EEA)
- Slovakia benefits from EU adequacy decision (within EEA)
- USA transfers (Stripe only) rely on Standard Contractual Clauses (SCCs) and supplementary technical measures

(f) LiveAgent Support System

- LiveAgent is hosted within the EU (Slovakia)
- Support tickets and communications are stored on LiveAgent's EU servers
- Customer Personnel data (name, email, account details) is processed for support purposes only
- Support ticket attachments may contain screenshots or data samples shared by the Customer for troubleshooting
- Retention: Support communications retained for 2 years for quality assurance and legal compliance
- Quality Unit (LiveAgent) complies with GDPR and maintains ISO 27001 certification

g) Sentry Error Tracking:

- Sentry provides error tracking and monitoring within EU data centers
- Error reports capture application errors and exceptions to ensure service reliability and identify issues
- Error data may include:
  - IP address
  - Device meta-data
  - Name
  - Email address
- Passwords and API keys are not stored in error logs
- Error logs are retained for 30 days, then automatically deleted
- Access to error logs is restricted to authorized Provider personal for debugging only

5.2 Sub-processor Changes

The Provider shall notify the Customer at least 14 days before adding or replacing any sub-processor in accordance with Clause 19.9.

5.3 Current Sub-processor List

An up-to-date list of sub-processors is available at https://support.wecouldeven.com/532022-Sub-processors-list or upon written request to support@wecouldeven.com.

5.4 Right to Object

In accordance with Clause 19.9(a)(ii), the Customer may object to the use of any sub-processor on reasonable data protection grounds within 14 days of notification. If the objection cannot be resolved and the Provider cannot provide Services without the sub-processor, the Customer may terminate without penalty with 30 days' notice.

6. Third Party Service Integrations and Data Flows

6.1 Engaging Networks Integration

When the Customer activates the Engaging Networks integration:

(a) Data Flow:

- Quiz participants complete quizzes on the Customer's quiz pages hosted by the Customer;s platform og choice
- Quiz responses (including participant Personal Data) are submitted to the Hosted Services
- The Provider's integration service, hosted on Fly.io infrastructure in the EU, transmits specified Personal Data to the Customer's Engaging Networks account via Engaging Networks' REST API
- Data transmission occurs a few minutes after quiz submission to ensure Engaging Networks API rate limits are not exceeded
- The Provider acts as a data processor transmitting data to another processor (Engaging Networks) on the Customer's documented instructions

(b) The types of Personal Data transmitted to Engaging Networks depend on the Customer's configuration, but may include:

- Name (first name, last name)
- Email address

- Phone number (if collected)
- Postcode/ZIP code (if collected)
- Quiz responses and scores
- Custom fields configured by the Customer
- Timestamp of submission
- Source/campaign identifiers
- Opt-in status of the quiz participant

(c) The Customer is solely responsible for:

i) ensuring it has a valid data processing agreement with Engaging Networks that complies with Data Protection Laws;

ii) ensuring it has lawful bases for collecting and transmitting Personal Data to Engaging Networks;

iii) obtaining any required consents from quiz participants for data transmission to Engaging Networks;

iv) configuring which Personal Data fields are transmitted to Engaging Networks;

v) compliance with Engaging Networks' terms of service and privacy policies;

vi) ensuring quiz participants are informed about data transmission to Engaging Networks in the Customer's privacy notice; and

vii) Engaging Networks' subsequent processing, storage, and use of Personal Data.

(d) The Provider:

i) processes Personal Data on the Customer's instructions when transmitting data to Engaging Networks;

ii) acts as the Customer's processor for the initial data collection and transmission;

iii) implements HTTPS/TLS encryption for all data transmitted to Engaging Networks;

iv) transmits only the data fields specified in the Customer's integration configuration;

v) does not control, monitor, or have visibility into Engaging Networks' processing of Personal Data after transmission;

vi) is not a party to the relationship between the Customer and Engaging Networks;
vii) is not responsible for Engaging Networks' data protection practices, security measures, or compliance with Data Protection Laws; and
viii) will cease transmission if the Customer deactivates the integration or upon the Customer's written instruction.

(e) Engaging Networks as Customer's Processor:
i) Engaging Networks is the Customer's chosen processor/sub-processor, not the Provider's sub-processor
ii) Engaging Networks does not appear in Section 5 (Sub-processors) because it processes data for the Customer, not for the Provider
iii) The Customer's data processing agreement with Engaging Networks governs that processing relationship
iv) Questions about Engaging Networks' data protection practices should be directed to Engaging Networks, not the Provider

(f) Transmission Security:
i) All data transmitted to Engaging Networks is encrypted using TLS 1.2 or higher
ii) API authentication uses secure methods (API keys, OAuth tokens)
iii) Transmission errors are logged and the Customer is notified
iv) The Provider does not store redundant copies of data transmitted to Engaging Networks (except as part of normal database operations in Supabase)
v) Integration infrastructure hosted on Fly.io uses isolated containers with encrypted storage and network traffic

(g) Geographic Considerations:
- Engaging Networks' data processing locations are determined by the Customer's Engaging Networks

account configuration
- The Customer is responsible for ensuring any international data transfers to Engaging Networks comply with Data Protection Laws
- The Provider is not responsible for transfers that occur within Engaging Networks' infrastructure

6.2 Future Third Party Service Integrations

(a) When additional Third Party Service integrations are added, similar data flow principles will apply:
- The Third Party Service is the Customer's processor, not the Provider's sub-processor
- The Customer is responsible for appropriate agreements and compliance
- The Provider acts as a technical conduit with secure transmission
- The Provider is not responsible for the Third Party Service's data protection practices

(b) Details of additional integrations will be documented in the Documentation and updated in this Schedule 4 as they become available.

6.3 Customer's Privacy Notice Obligations

The Customer must inform quiz participants in its privacy notice that:

- Personal Data collected through quizzes may be transmitted to third party services;
- which Third Party Services are being used (e.g., Engaging Networks);
- the purposes for which data is transmitted; and
- the Customer's lawful basis for such transmission.

The Provider's privacy policy covers the Provider's own processing only and does not cover Third Party Services chosen by the Customer.

7. Data Retention Periods

7.1 Customer Data Retention

(a) Active Accounts: Customer Data retained while the Customer's account remains active

(b) Terminated Accounts: Customer Data deleted or returned per Clause 12.6 and Clause 26.4 within 30 days of termination (unless Customer requests earlier deletion)

(c) Backups: Customer Data in backup systems is retained for 30 days from creation, then securely deleted

7.2 Support Communications Support tickets, chat transcripts, and related communications are retained for 2 years after ticket closure for quality assurance and legal compliance

7.3 System Logs and Analytics

(a) Security logs: 12 months for security incident investigation (manually stored for this period in the case of a security incident)

(b) Operational logs: up to 30 days

(c) Anonymized analytics: Retained indefinitely (no longer constitutes Personal Data under GDPR)

7.4 Transaction records and invoices retained for 7 years to comply with UK tax and accounting requirements (Companies Act 2006, Corporation Tax Act 2009)

7.5 The Provider may retain Personal Data beyond normal retention periods where required by law, to establish/defend legal claims, or upon receipt of legal hold notice

7.6 Data retention

(a) Quiz Respondent Data is retained for 30-60 days from collection. On the first day of each month, all Quiz Respondent Data collected more than 30 days prior is automatically and permanently deleted. Example: On March 1st, all data collected before February 1st is

deleted. Deletion is permanent and irreversible, rendering the data irrecoverable through normal system operations.

(b) The Provider shall notify the Customer approximately 7 days before the monthly deletion.

(c) The Customer is solely responsible for exporting data before monthly deletion.

(d) Quiz Respondent Data may be retained beyond the monthly deletion cycle only where:

(i) exported by the Customer to its own systems;

(ii) aggregated and anonymized (may be retained indefinitely per Section 7.3(c));

(iii) required by law or necessary for legal claims (Section 7.5); or

(iv) in backup systems (deleted per 30-day backup rotation per Section 7.1(c)).

(e) The Customer may export Quiz Respondent Data at any time before the monthly deletion through self-service tools (CSV format). Upon export, the Customer is solely responsible for: compliance with Data Protection Laws; implementing retention and deletion policies per GDPR Article 5(1)(e); responding to data subject requests; maintaining security; and breach notification. The Provider has no responsibility for exported data.

(f) Data subjects may exercise rights by contacting the Customer or Provider. The Provider shall forward requests to the Customer within 2 Business Days and provide assistance per Clause 19.10. After monthly deletion, the Provider cannot fulfill requests as data no longer exists. The Customer is solely responsible for requests relating to exported data.

(g) The Customer must inform quiz respondents in its privacy notice that: Personal Data is stored for 30-60 days; data is automatically deleted in monthly batches on the first day of each month; and rights may be exercised before deletion. The Provider shall include this in its Privacy Policy and Documentation.

(h) The Provider shall implement: accurate collection date tracking; reliable automated monthly deletion processes; verification of deletion completion; secure permanent deletion; and audit trails.

(i) The Provider shall display the age of Quiz Respondent Data in the Customer's dashboard, showing which data will be deleted in the next monthly batch.

8. Personal Data Breach Notification

In accordance with Clause 19.12 of the Agreement, if a Personal Data breach occurs affecting Customer Personal Data, the Provider shall notify the Customer within 24 hours, including:

8.1 Initial Notification (within 24 hours)

(a) Description of the nature of the breach
(b) Categories and approximate number of data subjects affected
(c) Categories and approximate number of Personal Data records affected
(d) Provider contact point for further information
(e) Likely consequences of the breach
(f) Immediate containment measures taken

8.2 Follow-up Information Where complete information cannot be provided immediately, the Provider shall provide updates every 24 hours until complete information is available, including:

(a) Root cause analysis
(b) Detailed timeline of the breach
(c) Complete list of affected data subjects (if determinable)
(d) Measures taken to address the breach and prevent recurrence
(e) Recommendations for the Customer's response
(f) Post-incident report (within 10 Business Days of resolution)

8.3 Customer Cooperation

The Provider shall fully cooperate with the Customer's investigation and any notifications the Customer must make to supervisory authorities or data subjects under GDPR Articles 33-34.

9. Automated Decision-Making and Profiling

9.1 The Hosted Services do not perform automated decision-making (including profiling) that produces legal effects concerning data subjects or similarly significantly affects them, within the meaning of Article 22 GDPR.

9.2 Quiz scoring and results are generated algorithmically based on quiz participant responses, but these do not constitute automated decision-making under Article 22 as they:

(a) are used by the Customer for informational and engagement purposes;
(b) do not produce legal effects or similarly significant effects; and
(c) remain under the Customer's control for any subsequent use.

9.3 If the Provider introduces any automated decision-making or profiling functionality in the future, the Provider shall notify Customers and update this Schedule accordingly.

10. Data Protection Impact Assessments

10.1 The Provider has conducted Data Protection Impact Assessments (DPIAs) for the following high-risk processing activities:

(a) International data transfers (Transfer Impact Assessment for Stripe payment processing in USA)

(b) Processing of special category personal data through quiz responses

10.2 The Provider reviews and updates DPIAs annually or when significant changes occur to processing activities.

10.3 Upon reasonable request, the Provider shall provide DPIA summaries (redacted for confidential information) to assist Customers with their own DPIA obligations under GDPR Article 35.

11. Records of Processing Activities

11.1 In accordance with Article 30(2) of the UK GDPR and EU GDPR, the Provider maintains records of processing activities carried out on behalf of Customers, containing:

(a) the name and contact details of the Provider and, where applicable, the Provider's data protection representative;

(b) the categories of processing carried out on behalf of each Customer;

(c) where applicable, transfers of Personal Data to third countries, including identification of those countries and documentation of appropriate safeguards; and

(d) a general description of technical and organisational security measures.

11.2 The Provider shall make its records of processing activities available to the Customer or supervisory authorities upon reasonable request, subject to redaction of information confidential to other customers.