Data Safety Policy for the "VPRYTUL" Mobile Application

This Data Safety Policy (the "Policy") is an internal and public document of the **SERHIY PRYTULA CHARITY FOUNDATION (EDRPOU code: 43720363)** (hereinafter referred to as the "Foundation" or "Data Controller"). The document outlines the specific technical, engineering, and organizational measures implemented to protect the Personal Data of users of the "VPRYTUL" mobile application and the official website www.vprytul.app (collectively, the "Service"), in compliance with the Law of Ukraine "On Personal Data Protection," the European GDPR, and the US CCPA.

1. Organizational Security Measures
The Foundation enforces strict internal access controls for users' Personal Data:
1.1. Principle of Least Privilege: Access to the user database and admin panel is granted exclusively to a limited number of Foundation employees who require this information to perform their job duties (e.g., Technical Administrator, Communications Lead).
1.2. Non-Disclosure Agreements (NDA): All Foundation employees and engaged specialists with access to Personal Data have signed personal confidentiality agreements committing them not to disclose information to third parties.
1.3. Logging and Auditing: Any administrator actions within the system (e.g., viewing data, changing statuses, approving quests) are automatically recorded in security system logs. This allows us to track exactly who accessed the information and when.

2. Technical and Engineering Security Measures
To ensure data confidentiality and integrity, we utilize a modern security technology stack:
2.1. Data in Transit Encryption: All interactions between the user's device (the mobile app or web browser on the Site www.vprytul.app) and the backend servers are protected by the TLS/SSL cryptographic protocol using automatically validated SSL certificates (Amazon Issued). Data interception over networks is technically impossible.
2.2. Data at Rest Encryption: Databases and file storages containing user information are encrypted using the AES-256 standard at the cloud infrastructure level.
2.3. Anti-Brute Force Protection: Registration and authorization processes are protected by algorithms that prevent automated guessing of email addresses or phone numbers (protecting the login flow from external scanning).

3. Register of Authorized Sub-processors and Third Parties
To ensure stable technical operations, send notifications, and process payments, the Foundation engages reliable third-party services (Data Processors / Sub-processors). Data transmission is executed strictly within the scope necessary to perform a specific technical function.

Sub-processor / Service	Role and Function in the Project	Categories of Data Transferred	Security Measures and Processing Location

Microsoft Azure	Cloud infrastructure, database, and app server hosting managed by the **SERHIY PRYTULA CHARITY FOUNDATION (EDRPOU code: 43720363)**.	All user profiles (email, name, phone number), geolocation, quest logs, and device analytics.	Servers are located in secure EU data centers (West Europe / North Europe regions and others). AES-256 encryption, network isolation (Virtual Network / Network Security Groups), ISO 27001, SOC 1/2/3 certifications.
Qela Inc.	Platform vendor (White-label developer). Provides technical support, code updates, and debugging at the request of the **SERHIY PRYTULA CHARITY FOUNDATION**	Access to backend technical logs during troubleshooting (without the right to independent use or copying of databases).	Access is governed by a Data Processing Agreement (DPA). Restricted access via secure IAM roles exclusively on the servers of the **SERHIY PRYTULA CHARITY FOUNDATION**.
LiqPay (JSC CB PrivatBank)	Payment gateway for one-time donations and monthly recurring subscriptions.	Phone number, email, donation amount, unique transaction ID. Important: payment card data is entered on the bank's secure page and is not collected by the **SERHIY PRYTULA CHARITY FOUNDATION**	Data centers in Ukraine/EU. Full compliance with the international Payment Card Industry Data Security Standard (PCI DSS).

SendGrid (Twilio Inc.)	Automated transactional email service (sending welcome emails and registration confirmations).	Email address, user's name (for personalizing system emails).	TLS encryption in transit. Data centers in the US/EU compliant with GDPR / Privacy Shield standards.
Google LLC — Gmail SMTP	Sending transactional emails (User portal, MobileHost).	Recipient's email address, name, and email content.	US; TLS encryption in transit; Google Cloud DPA.
Google LLC — Firebase Cloud Messaging	Delivery of push notifications (backend-initiated, Android and iOS clients).	FCM push token, Device ID, notification content, UserId, IP address.	US / global Google infrastructure; encryption in transit; Firebase Terms / Google Cloud DPA.
Google LLC — Firebase Crashlytics	Collection of app crash reports (Android, iOS).	Device model, OS/app version, stack trace, Device ID, IP address.	US; Firebase Terms / Google Cloud DPA.

Google LLC — Firebase App Check	Protection of API requests from abuse/bot traffic via device attestation (iOS).	Technical device attestation token, Device ID.	US / global Google infrastructure; Firebase Terms / Google Cloud DPA.
Google LLC — Google Maps Platform	Map display, geocoding, and geolocation for geo-quests and delivery addresses (Android, iOS).	GPS coordinates, IP address, entered address, Device ID.	US / EU; Google Maps Platform Terms / Google Cloud DPA.
Google LLC — Google Sign-In / Identity Services	Authentication via Google account (backend, Android, iOS).	Email address, name, Google User ID / ID token, profile picture, OAuth tokens.	US / EU; Google API Services User Data Policy / Google Cloud DPA.
Google LLC — YouTube Player (IFrame Player / YouTubePlayerKit)	Video playback in quests (Android, iOS).	IP address, Device ID, viewing data.	US; YouTube API Services Terms / Google Privacy Policy.

Google LLC — Google Play Services (App Update API, Advertising ID)	Enforcement of app updates; device advertising identifier (Android).	Advertising ID (AD_ID), app version.	US; Google Play Services Terms.
Microsoft Azure — App Service (Backend/API Hosting)	Hosting of the app's API/backend.	All Personal Data passing through the API — profile data, phone number, email address, and content.	West Europe; HTTPS/TLS encryption in transit; Microsoft Products and Services DPA.
Microsoft Azure Blob Storage	Storage of user-uploaded files/images.	User files/photos associated with UserId/OrganizationId.	West Europe; encryption at rest; Microsoft Products and Services DPA.
Microsoft Azure Key Vault	Storage of encryption keys for the DataProtection keyring.	Does not directly store Personal Data — only the cryptographic keys used to protect Personal Data.	West Europe; provider's hardware HSM module; Microsoft Products and Services DPA.

Azure DevOps (Microsoft Corporation)	CI/CD — building and storing app artifacts.	Does not directly process users' Personal Data — only source code/build artifacts.	West Europe; Microsoft Products and Services DPA.
Apple Inc. — Sign in with Apple	Authentication via Apple ID (iOS app + backend token validation).	Email address (possibly an Apple Private Relay address), Apple User ID (sub).	US; token signature verified via Apple's public keys; Apple Developer Agreement.
Nova Poshta (AT «Нова Пошта»)	Selection of a delivery address/branch for store merchandise.	City/delivery address, branch number.	Ukraine; Nova Poshta Public Offer Agreement.
SignalR Backend (сервер реального часу)	Real-time messaging and data synchronization.	User ID, Organization ID, messages, service events, technical logs.	Within the infrastructure of the **SERHIY PRYTULA CHARITY FOUNDATION (EDRPOU code: 43720363)**; Internal Data Processing Agreement (DPA).

Backend API (через Alamofire/Moya)	Execution of app business logic and processing of API requests.	Account data, User ID, Organization ID, and Personal Data transmitted via the API.	Within the infrastructure of the **SERHIY PRYTULA CHARITY FOUNDATION (EDRPOU code: 43720363)**; Internal Data Processing Agreement (DPA).

4. Data Breach Protocol

The Foundation has a clear action plan in the event of a cyber threat or unauthorized access to our servers:

4.1. Isolation and Containment: Upon detecting a breach attempt, the technical team immediately blocks compromised sessions, isolates the affected segments of the AWS servers, and terminates any suspicious processes.

4.2. Investigation: Within the first few hours, a detailed technical audit of the logs is conducted to determine the scope of the incident.

4.3. Notification (72-Hour Rule): If a risk of a Personal Data breach that could harm users is identified, the Foundation commits to the following within 72 hours of becoming aware of the incident:

- Notify the Ukrainian Parliament Commissioner for Human Rights (or the relevant Data Protection Authorities in the EU if the incident affects EU residents);
- Send official email notifications to the affected users with clear instructions (e.g., a recommendation to update passwords).

5. Policy Control and Updates

5.1. This Policy is reviewed at least once a year, as well as whenever new technical integrations are implemented, payment gateways are changed, or the app's cloud architecture is updated.

5.2. The current version of this document is always available in digital format for the Foundation's internal IT team and legal department.