Політика захисту даних мобільного застосунку «Впритул» (VPRYTUL)

Ця Політика захисту даних (далі – «Політика») є внутрішнім та публічним документом БО « ФОНД СЕРГІЯ ПРИТУЛИ» (код ЄДРПОУ: 43720363, далі — «Фонд» або «Контролер»). Документ визначає конкретні технічні, інженерні та організаційні заходи, що вживаються для захисту персональних даних користувачів мобільного застосунку «Впритул» (VPRYTUL) та офіційного вебсайту www.vprytul.app (далі разом – «Сервіс»), відповідно до Закону України «Про захист персональних даних», європейського регламенту GDPR та американського CCPA.

1. Організаційні заходи безпеки
Фонд впроваджує суворий контроль внутрішнього доступу до персональних даних користувачів:
1.1. **Принцип мінімальних привілеїв:** Доступ до бази даних користувачів та панелі адміністратора надається виключно обмеженому колу працівників Фонду, яким ця інформація необхідна для виконання посадових обов'язків (Технічний адміністратор, Комунікаційний лід).
1.2. **Зобов'язання про нерозголошення (NDA):** Усі співробітники та залучені спеціалісти Фонду, які мають доступ до персональних даних, підписали персональні зобов’язання щодо конфіденційності та нерозголошення інформації третім особам.
1.3. **Логування та аудит:** Будь-які дії адміністраторів у системі (перегляд даних, зміна статусів, апрув квестів) автоматично фіксуються в системних логах безпеки. Це дозволяє відстежувати, хто саме і коли мав доступ до інформації.

2. Технічні та інженерні заходи захисту
Для забезпечення конфіденційності та цілісності даних застосовується сучасний стек технологій безпеки:
2.1. **Шифрування під час передачі (Data in Transit):** Уся взаємодія між пристроєм користувача (мобільним застосунком чи веббраузером на Сайті www.vprytul.app) та серверною частиною захищена криптографічним протоколом TLS/SSL за допомогою автоматично валідованих SSL-сертифікатів (Amazon Issued). Перехоплення даних у мережах є технічно неможливим.
2.2. **Шифрування під час зберігання (Data at Rest):** Бази даних та файлові сховища, де міститься інформація користувачів, шифруються за стандартом AES-256 на рівні хмарної інфраструктури.
2.3. **Захист від перебору (Анти-брутфорс):** Процеси реєстрації та авторизації захищені алгоритмами, які унеможливлюють автоматизований підбір електронних адрес або номерів телефонів (захист флоу логіну від зовнішнього сканування).

3. Реєстр авторизованих субпроцесорів та третіх сторін
Для забезпечення стабільної технічної роботи, надсилання сповіщень та обробки платежів Фонд залучає надійні сторонні сервіси (субпроцесори). Передача даних здійснюється виключно в обсязі, необхідному для виконання конкретної технічної функції.

Контрагент / Сервіс	Роль та функція в проєкті	Категорії даних, що передаються	Заходи безпеки та місце обробки
Amazon Web Services (AWS)	Хмарна інфраструктура, хостинг баз даних та серверів застосунку під управлінням Фонду.	Усі профілі користувачів (email, ім'я, телефон), геолокація, логі квестів та аналітика пристрою.	Сервери розташовані в захищених дата-центрах ЄС. Шифрування AES-256, ізоляція мереж, сертифікація ISO 27001, SOC 1/2/3.
Qela Inc.	Вендор платформи (White Label розробник). Здійснює технічну підтримку, оновлення коду та дебаг за запитом Фонду.	Доступ до технічних логів бекенду під час усунення помилок (без права власного використання чи копіювання баз даних).	Доступ регулюється Договором про обробку даних (DPA). Обмежений доступ через захищені IAM-ролі виключно на серверах Фонду.
LiqPay (АТ КБ «ПриватБанк»)	Платіжний шлюз для разових донатів та щомісячних рекурентних підписок.	Номер телефону, email, сума внеску, унікальний ID транзакції. **Важливо:** дані платіжних карток вводяться на захищеній сторінці банку і Фондом не збираються.	Дата-центри в Україні/ЄС. Повна відповідність міжнародному стандарту безпеки банківських карток PCI-DSS.

SendGrid (Twilio Inc.)	Сервіс автоматизованих транзакційних імейлів (надсилання вітальних листів, підтверджень реєстрації).	Електронна пошта (email), ім'я користувача (для персоналізації системного листа).	Шифрування TLS під час передачі листів. Дата-центри в США/ЄС із захистом за стандартами GDPR / Privacy Shield.
Google LLC (Gmail SMTP)	Надсилання транзакційних email (User-портал, MobileHost)	Email-адреса отримувача, ім'я, вміст листа	
Google LLC — Gmail SMTP	Надсилання транзакційних email (User-портал, MobileHost)	Email-адреса отримувача, ім'я, вміст листа	США; TLS-шифрування з'єднання; Google Cloud DPA
Google LLC — Firebase Cloud Messaging	Доставка push-сповіщень (бекенд-ініціація, Android і iOS клієнти)	FCM push-токен, ідентифікатор пристрою, вміст сповіщення, UserId, IP-адреса	США / глобальна інфраструктура Google; шифрування каналу; Firebase Terms / Google Cloud DPA

Google LLC — Firebase Crashlytics	Збір звітів про збої застосунку (Android, iOS)	Модель пристрою, версія ОС/застосунку, stack trace, ідентифікатор пристрою, IP-адреса	США; Firebase Terms / Google Cloud DPA
Google LLC — Firebase App Check	Захист API-запитів від зловживань/бот-трафіку через атестацію пристрою (iOS)	Технічний токен атестації пристрою (device attestation token), ідентифікатор пристрою	США / глобальна інфраструктура Google; Firebase Terms / Google Cloud DPA
Google LLC — Google Maps Platform	Відображення карт, геокодування, геолокація для геоквестів та адрес доставки (Android, iOS)	GPS-координати, IP-адреса, введена адреса, ідентифікатор пристрою	США / ЄС; Google Maps Platform Terms / Google Cloud DPA
Google LLC — Google Sign-In / Identity Services	Автентифікація через Google-акаунт (бекенд, Android, iOS)	Email, ім'я, Google User ID / ID token, фото профілю, OAuth-токени	США / ЄС; Google API Services User Data Policy / Google Cloud DPA

Google LLC — YouTube Player (IFrame Player / YouTubePlayerKit)	Відтворення відео у квестах (Android, iOS)	IP-адреса, ідентифікатор пристрою, дані перегляду	США; YouTube API Services Terms / Google Privacy Policy
Google LLC — Google Play Services (App Update API, Advertising ID)	Примусове оновлення застосунку; рекламний ідентифікатор пристрою (Android)	Advertising ID (AD_ID), версія застосунку	США; Google Play Services Terms
Microsoft Azure — App Service (хостинг бекенду/API)	Хостинг API/бекенду застосунку	Усі персональні дані, що проходять через API — профіль, телефон, email, контент	West Europe; HTTPS/TLS; Microsoft Products and Services DPA
Microsoft Azure Blob Storage	Зберігання файлів/зображень, завантажених користувачами	Файли/фото користувача, пов’язані з UserId/OrganizationId	West Europe; шифрування при зберіганні; Microsoft Products and Services DPA

Microsoft Azure Key Vault	Зберігання ключів шифрування DataProtection keyring	Напряму ПД не зберігає — лише криптографічні ключі, що захищають ПД	West Europe; апаратний HSM-модуль провайдера; Microsoft Products and Services DPA
Azure DevOps (Microsoft Corporation)	CI/CD — збірка та зберігання артефактів застосунку	ПД користувачів напряму не обробляє — лише вихідний код/білд-артефакти	West Europe; Microsoft Products and Services DPA
Stripe	Обробка платежів (поповнення балансу організації)	Email платника, дані картки (маскований last4), сума транзакції, ID замовлення	США; PCI DSS на стороні Stripe, дані картки не зберігаються застосунком; Stripe DPA
Apple Inc. — Sign in with Apple	Автентифікація через Apple ID (iOS-застосунок + бекенд-валідація токена)	Email (можливо приватний relay-адрес Apple), Apple User ID (sub)	США; підпис токена перевіряється публічними ключами Apple; Apple Developer Agreement

Nova Poshta (АТ «Нова Пошта»)	Підбір адреси/відділення для доставки товарів магазину	Місто/адреса доставки, номер відділення	Україна; Договір-оферта Nova Poshta
SignaIR Backend (сервер реального часу)	Обмін повідомленнями в режимі реального часу, синхронізація даних	User ID, Organization ID, повідомлення, службові події, технічні журнали	Відповідно до інфраструктури компанії; Внутрішній DPA / Data Processing Agreement
Backend API (через Alamofire/Moya)	Виконання бізнес-логіки застосунку, обробка API-запитів	Дані облікового запису, User ID, Organization ID, персональні дані, що передаються API	Відповідно до інфраструктури компанії; Внутрішній DPA / Data Processing Agreement

4. Протокол дій у разі інцидентів (Data Breach Protocol)
Фонд має чіткий алгоритм дій на випадок виникнення кіберзагрози або несанкціонованого доступу до серверів:
4.1. **Ізоляція та фіксація:** У разі виявлення спроби злому, технічна команда негайно блокує скомпрометовані сесії, ізолює пошкоджені сегменти серверів AWS та зупиняє підозрілі процеси.
4.2. **Розслідування:** Протягом перших годин проводиться детальний технічний аудит логів для встановлення масштабів інциденту.
4.3. **Повідомлення (Правило 72 годин):** Якщо виявлено ризик витоку персональних даних, який може зашкодити користувачам, Фонд зобов'язується протягом 72 годин з моменту встановлення факту інциденту:

- Сповістити про це Уповноваженого Верховної Ради України з прав людини (або відповідні органи захисту даних в ЄС, якщо інцидент торкнувся резидентів ЄС);
- Надіслати офіційні повідомлення електронною поштою постраждалим користувачам із чіткими інструкціями (наприклад, рекомендацією оновити паролі).

5. Контроль та оновлення Політики

5.1. Ця Політика переглядається щонайменше один раз на рік, а також щоразу при впровадженні нових технічних інтеграцій, зміні платіжних шлюзів або оновленні хмарної архітектури застосунку.

5.2. Поточна версія документа завжди доступна в електронному вигляді для внутрішньої IT-команди та юридичного департаменту Фонду.