Політика конфіденційності

Затверджено 16 грудня 2024 року
адміністрацією AlgoWizzards
для платформи FarmsteadHelper

Розділ 1. Вступ

1.1. Мета Політики конфіденційності

1. **Прозорість обробки даних:** Політика покликана пояснити користувачам, як платформа збирає, використовує та зберігає їхні дані. Це включає обґрунтування причин збору кожного типу даних.
2. **Забезпечення довіри:** Користувачі повинні бути впевнені, що їхні дані захищені від несанкціонованого доступу або використання.
3. **Юридичний обов'язок:** Виконання вимог законодавства щодо конфіденційності даних є однією з основних цілей політики. Платформа зобов’язується діяти в рамках законів і регламентів, які регулюють захист персональних даних.
4. **Захист прав користувачів:** Політика спрямована на інформування користувачів про їхні права щодо управління своїми даними, а також про способи реалізації цих прав.
5. **Підтримка функціональності платформи:** Дані користувачів необхідні для забезпечення належної роботи сервісів платформи, таких як реєстрація, сповіщення, персоналізація тощо.

1.2. Правова основа

1. **GDPR та міжнародне законодавство:** Платформа зобов’язується дотримуватися положень Загального регламенту захисту даних (GDPR) Європейського Союзу, що є ключовим стандартом у захисті персональних даних.
2. **Законодавство України:** Платформа також дотримується Закону України "Про захист персональних даних", який регулює обробку інформації всередині країни.
3. **Адаптація до міжнародних стандартів:** Якщо користувач знаходиться в іншій країні, платформа враховує специфіку законодавства щодо конфіденційності даних цієї країни.

1.3. Застосування Політики

1. **Сфера дії:** Політика поширюється на всіх користувачів, які реєструються або взаємодіють із платформою. Це включає як основний вебсайт, так і мобільні додатки.

2. **Охоплення:** Усі види даних, які збираються автоматично (через cookies) або вводяться користувачем вручну, підпадають під дію цієї Політики.
3. **Діяльність третіх сторін:** Політика не охоплює сторонні сервіси, з якими платформа взаємодіє, якщо ці сервіси мають свої власні умови конфіденційності.

1.4. Визначення термінів

1. **"Персональні дані":** Інформація, яка прямо чи опосередковано ідентифікує користувача (наприклад, ім'я, електронна адреса, номер телефону).
2. **"Обробка даних":** Дії, що здійснюються з персональними даними, включаючи збір, зберігання, аналіз, передачу, видалення тощо.
3. **"Cookies":** Невеликі текстові файли, які зберігаються на пристрої користувача для забезпечення його ідентифікації на платформі.

1.5. Зобов’язання платформи

1. **Обмеження обсягу даних:** Платформа збирає лише ті дані, які є необхідними для функціонування сервісів.
2. **Захист конфіденційності:** Всі зібрані дані обробляються з урахуванням стандартів безпеки, щоб мінімізувати ризик витоку чи несанкціонованого доступу.
3. **Дотримання прав користувачів:** Адміністрація платформи гарантує швидке реагування на запити користувачів щодо їхніх даних.

1.6. Умови прийняття Політики

1. **Погодження:** Реєстрація або використання платформи автоматично означає, що користувач ознайомлений з Політикою конфіденційності і згоден з нею.
2. **Зобов’язання користувача:** Користувач зобов’язаний не порушувати положення Політики конфіденційності під час взаємодії з платформою.

1.7. Інформування користувачів

1. **Сповіщення про зміни:** Усі оновлення Політики будуть повідомлятися через електронну пошту або повідомлення на платформі.
2. **Доступ до документа:** Політика конфіденційності доступна для перегляду в будь-який момент через спеціальний розділ платформи.

1.8. Межі відповідальності

1. **Обмеження зобов’язань:** Адміністрація платформи не несе відповідальності за дії користувачів, які призвели до порушення конфіденційності їхніх даних (наприклад, публічний розголос паролю).
2. **Сторонні сервіси:** У разі використання сервісів третіх сторін відповідальність за їхню конфіденційність покладається на цих постачальників послуг.

1.9. Мова документа

1. **Основна мова:** Політика конфіденційності публікується українською мовою. У разі суперечностей між версіями на інших мовах перевага надається україномовній версії.
2. **Додаткові переклади:** Адміністрація залишає за собою право надавати переклади Політики іншими мовами.

1.10. Контактна інформація

1. **Засоби комунікації:** Для зв’язку з адміністрацією можна скористатися формою зворотного зв’язку на платформі або надіслати електронний лист за вказаною адресою.
2. **Графік обробки запитів:** Усі запити щодо конфіденційності обробляються в робочий час, протягом 20 робочих днів.

Розділ 2. Збір даних

2.1. Категорії даних

1. **Особисті дані:**
    - Ідентифікаційні дані: ім'я, прізвище, псевдонім, дата народження.
    - Контактні дані: електронна адреса.
    - Дані, пов’язані з акаунтом: логін, пароль (у зашифрованому вигляді), аватар.
2. **Технічні дані:**
    - IP-адреса, яка використовується для входу на платформу.
    - Дані про пристрій (модель, операційна система, тип браузера).
    - Інформація про роздільну здатність екрана.
3. **Аналітичні дані:**
    - Дані про поведінку користувача на платформі (які сторінки відвідував, час перебування).
    - Інтеракції з контентом (клікання на кнопки, прокрутка сторінок).
    - Джерело переходу на платформу (посилання, реклама, пошукова система).

2.2. Джерела збору даних

1. **Безпосереднє введення:**
    - Дані, які користувач вводить під час реєстрації, заповнення профілю або надсилання запитів.
2. **Автоматичний збір:**
    - Дані, які збираються через cookies, аналітичні сервіси, або логи серверів.
3. **Дані від третіх сторін:**
    - Інформація, яку платформа отримує через інтеграції (наприклад, авторизація через соціальні мережі).

2.3. Файли cookies

1. **Функціональні cookies:**
    - Використовуються для забезпечення роботи платформи (авторизація, збереження налаштувань).
2. **Аналітичні cookies:**
    - Використовуються для оцінки поведінки користувачів, що дозволяє платформі оптимізувати свої сервіси.
3. **Рекламні cookies:**
    - Використовуються для персоналізації реклами та вимірювання ефективності маркетингових кампаній.

2.4. Цілі збору даних

1. **Надання послуг:**
    - Реєстрація акаунтів, авторизація, виконання замовлень.
2. **Персоналізація:**
    - Адаптація контенту та функціоналу під конкретного користувача.
3. **Комунікація:**
    - Надсилання важливих повідомлень, сповіщень, оновлень про платформу.

2.5. Способи збору даних

1. **Ручне введення:**
    - Форми реєстрації, заявки на участь у подіях, запити через службу підтримки.
2. **Автоматизовані механізми:**
    - Аналітичні сервіси (наприклад, Google Analytics), інструменти відстеження активності користувачів.
3. **API-інтеграції:**
    - Дані, отримані через сторонні платформи або сервіси.

2.6. Законність збору даних

1. **Згода користувача:**
    - Дані збираються тільки після явної згоди користувача (наприклад, через прийняття Політики).
2. **Юридична необхідність:**
    - Дані можуть збиратися, якщо це вимагається законом (наприклад, для звітності).
3. **Законний інтерес:**
    - Збір даних для поліпшення послуг або забезпечення безпеки.

2.7. Відмова від надання даних

1. **Добровільність:**
    - Користувач має право не надавати персональні дані, але це може обмежити доступ до функцій платформи.
2. **Мінімальні вимоги:**
    - Для основної роботи платформи потрібні лише базові дані (логін, електронна пошта, ім’я, прізвище).

2.8. Спеціальні категорії даних

1. **Чутливі дані:**
    - Платформа не збирає інформацію про расу, релігію, політичні погляди або стан здоров’я.

2.9. Право на відмову від збору даних

1. **Блокування cookies:**
    - Користувачі можуть відключити cookies у налаштуваннях браузера.
2. **Обмеження збору:**
    - Користувач може вимагати зупинити обробку даних через звернення до адміністрації.

Розділ 3. Використання даних

3.1. Основні цілі використання даних

1. **Реєстрація та управління акаунтом:**
    - Використання імені, електронної адреси, та пароля для створення акаунту.
    - Забезпечення функцій для відновлення доступу до акаунту.
2. **Надання послуг:**
    - Обробка даних для надання основних сервісів платформи, таких як створення профілів, розміщення контенту, доступ до функцій.
3. **Персоналізація:**
    - Використання аналітичних даних для адаптації інтерфейсу, відображення релевантного контенту, рекомендацій або налаштувань.
4. **Забезпечення комунікації:**
    - Надсилання сповіщень про оновлення, повідомлень адміністрації, інформаційних бюлетенів.

3.2. Внутрішня аналітика та статистика

1. **Оптимізація роботи платформи:**
    - Використання зібраних даних для виявлення проблем у роботі сайту, таких як помилки або повільне завантаження сторінок.
2. **Покращення функціоналу:**
    - Аналіз поведінки користувачів для вдосконалення існуючих послуг або розробки нових.
3. **Оцінка популярності контенту:**
    - Визначення, який контент є найбільш затребуваним серед користувачів.
4. **Звітність:**
    - Створення внутрішніх звітів для аналізу ефективності роботи сервісів.

3.3. Безпека та запобігання шахрайству

1. **Виявлення підозрілої активності:**
    - Аналіз логів для виявлення незвичайної активності, що може вказувати на злом акаунтів.
2. **Запобігання спам-атакам:**
    - Використання IP-даних і поведінкових моделей для блокування ботів і спамерів.
3. **Юридичне забезпечення:**
    - Використання даних для відповідності законодавству та захисту прав платформи.

3.4. Маркетинг і реклама

1. **Персоналізація реклами:**
    - Використання аналітичних даних для відображення таргетованої реклами.
2. **Взаємодія з партнерами:**
    - Надання зведених даних партнерам для оцінки ефективності рекламних кампаній.

3.5. Комунікація з користувачами

1. **Оновлення умов:**
    - Надсилання повідомлень про зміни в Політиці конфіденційності або Умовах користування.
2. **Інформування про нові послуги:**
    - Повідомлення про нові функції платформи або акції.

3.6. Використання даних для правових цілей

1. **Розгляд скарг:**
    - Використання персональних даних для вирішення суперечок із користувачами.

2. **Виконання юридичних вимог:**
    - Надання даних державним органам у рамках законодавства.

3.7. Агрегація та анонімізація даних

1. **Створення статистичних моделей:**
    - Використання агрегованих даних для створення загальної статистики без прив’язки до конкретного користувача.
2. **Анонімізація:**
    - Перетворення даних у формат, який не дозволяє ідентифікувати користувача.

3.8. Права користувачів при обробці даних

1. **Запит на інформацію:**
    - Користувач має право дізнатися, як використовуються його дані.
2. **Заперечення:**
    - Користувач може висловити заперечення проти використання його даних у певних цілях, таких як маркетинг.

3.9. Відмова від певних видів використання

1. **Налаштування реклами:**
    - Користувач може відмовитися від персоналізованої реклами через налаштування.
2. **Відключення cookies:**
    - Забезпечується механізм для відключення певних типів cookies.

3.10. Інформаційна прозорість

1. **Публічність:**
    - Уся інформація про використання даних викладена у цій Політиці.
2. **Доступність:**
    - Політика доступна в будь-який час через посилання внизу сторінки платформи.

Розділ 4. Зберігання даних

4.1. Локація зберігання даних

1. **Фізичне розташування серверів:**
    - Дані користувачів зберігаються на серверах у регіонах, де діють відповідні закони про захист даних (наприклад, у країнах ЄС відповідно до GDPR).
    - Компанія використовує дата-центри, сертифіковані відповідно до міжнародних стандартів безпеки.
2. **Хмарні рішення:**
    - Частина даних може зберігатися у сертифікованих хмарних сховищах (наприклад, Amazon AWS, Google Cloud).
    - Хмарні провайдери обрані на основі їх репутації та відповідності вимогам безпеки.
3. **Резервне копіювання:**
    - Резервні копії даних створюються регулярно та зберігаються в окремих захищених локаціях для відновлення інформації у разі технічних збоїв.
4. **Локалізація даних:**
    - Якщо законодавство окремих країн вимагає зберігання даних на території країни користувача, платформа дотримується цих вимог.

4.2. Принципи організації зберігання даних

1. **Мінімізація даних:**
    - Збираються лише ті дані, які необхідні для надання послуг.
    - Дані, які більше не потрібні, видаляються або анонімізуються.
2. **Сегментація даних:**
    - Різні категорії даних (наприклад, особисті, технічні, фінансові) зберігаються у відокремлених базах.

3. **Шифрування:**

- Дані шифруються як під час зберігання, так і під час передачі між серверами (з використанням TLS/SSL).

4. **Контроль доступу:**
    - Доступ до баз даних мають лише авторизовані співробітники, що пройшли відповідну перевірку.
    - Використовуються системи багаторівневої автентифікації.

4.3. Термін зберігання даних

1. **Персональні дані:**
    - Зберігаються протягом дії облікового запису користувача.
    - Після видалення облікового запису дані знищуються через 30 днів, якщо інше не передбачено законом.
2. **Технічні дані:**
    - Логи сервера зберігаються протягом 6 місяців для діагностики проблем.
    - Дані cookies зберігаються відповідно до їхньої функціональності (наприклад, 1 рік для налаштувань користувача).
3. **Дані для аналітики:**
    - Агреговані та анонімізовані дані можуть зберігатися без обмеження терміну.
4. **Юридичні обмеження:**
    - Якщо закон вимагає зберігання певної інформації (наприклад, фінансових транзакцій) протягом конкретного періоду, платформа дотримується таких вимог.

4.4. Захист даних від втрати

1. **Системи резервного копіювання:**
    - Щоденне резервне копіювання зберігається у зашифрованому вигляді на віддалених серверах.
    - Платформа проводить регулярне тестування системи відновлення даних.
2. **Захист від збоїв:**

- Використовуються системи RAID для зберігання даних із надлишковістю.
- Сервери захищені від відмови обладнання, забезпечуючи постійний доступ до даних.

4.5. Видалення даних

1. **Автоматичне видалення:**
   - Дані видаляються автоматично після закінчення терміну зберігання.
2. **Видалення на запит:**
   - Користувачі мають право подати запит на видалення своїх даних, який обробляється протягом 30 днів.
3. **Анонімізація даних:**
   - Замість видалення певні дані можуть бути анонімізовані, щоб більше не асоціюватися з конкретним користувачем.

4.6. Захист від несанкціонованого доступу

1. **Фізична безпека:**
   - Сервери розташовані у захищених дата-центрах з доступом лише для авторизованого персоналу.
2. **Віртуальна безпека:**
   - Використання міжмережевих екранів і захищених протоколів для мінімізації ризику злому.
3. **Моніторинг:**
   - Постійний моніторинг активності на серверах для виявлення та запобігання підозрілій активності.

4.7. Прозорість зберігання даних

1. **Інформування користувачів:**
   - У Політиці конфіденційності вказуються всі аспекти зберігання даних.

2. **Оновлення інформації:**

- Будь-які зміни у способах зберігання даних публікуються та повідомляються користувачам.

4.8. Обробка запитів від користувачів

1. **Доступ до інформації:**
   - Користувач може подати запит на отримання інформації про те, як зберігаються його дані.
2. **Уточнення чи виправлення:**
   - Користувач може вимагати виправлення або оновлення своїх даних.

4.9. Аудит і перевірки зберігання даних

1. **Внутрішній аудит:**
   - Регулярна перевірка баз даних для забезпечення їх відповідності стандартам безпеки.
2. **Зовнішній аудит:**
   - Періодична перевірка незалежними організаціями на предмет безпеки та відповідності законодавству.

4.10. Політика у разі порушення безпеки

1. **Оповіщення:**
   - Користувачі негайно повідомляються у разі виявлення витоку даних.
2. **Відновлення:**
   - Активуються плани з відновлення, щоб мінімізувати наслідки порушення.
3. **Звітність:**
   - Інцидент документується та аналізується для запобігання подібним ситуаціям у майбутньому.

Розділ 5. Розкриття даних третім сторонам

5.1. Загальні принципи передачі даних

1. **Законна основа передачі:**
    - Дані передаються лише у випадках, передбачених законодавством (наприклад, на підставі договору, згоди користувача або юридичних вимог).
2. **Прозорість:**
    - Користувачі інформуються про передачу даних через Політику конфіденційності або окреме повідомлення.
3. **Мінімізація даних:**
    - Передаються лише ті дані, які є необхідними для конкретної мети.
4. **Безпека передачі:**
    - Передача здійснюється із застосуванням шифрування та інших захисних заходів.
5. **Контроль над даними:**
    - Платформа забезпечує, щоб треті сторони використовували дані лише відповідно до умов договору та Політики конфіденційності.

5.2. Розкриття даних партнерам

1. **Типи партнерів:**
    - Дані можуть передаватися партнерам, які надають сервіси, пов’язані з роботою платформи (наприклад, платіжні системи, постачальники хостингу, служби доставки).
2. **Цілі співпраці:**
    - Передача здійснюється для реалізації основних функцій платформи (обробка платежів, надсилання повідомлень тощо).
3. **Договірні зобов'язання:**
    - Усі партнери підписують угоду, яка передбачає дотримання норм захисту даних.

4. **Обмеження використання:**
    - Партнери не мають права використовувати дані для власних цілей без прямої згоди користувача.

5.3. Розкриття даних рекламодавцям

1. **Агреговані дані:**
    - Дані передаються в узагальненій або анонімізованій формі для статистичних цілей.
2. **Персоналізована реклама:**
    - У разі надання згоди користувача, дані можуть використовуватися для персоналізації реклами.
3. **Відмова від реклами:**
    - Користувач може відмовитися від отримання персоналізованої реклами через налаштування облікового запису.
4. **Контроль над рекламодавцями:**
    - Платформа проводить перевірку рекламодавців перед початком співпраці.

5.4. Розкриття даних юридичним особам

1. **Юридичні вимоги:**
    - Дані можуть передаватися на запит державних органів відповідно до закону.
2. **Судові процеси:**
    - У разі участі у судовому процесі, дані користувача можуть бути надані як доказ.
3. **Обмеження доступу:**
    - Передача здійснюється лише в обсязі, необхідному для виконання юридичних вимог.
4. **Інформування користувачів:**
    - У разі, якщо це не суперечить закону, користувачів повідомляють про передачу їхніх даних.

5.5. Передача даних міжнародним партнерам

1. **Юрисдикції:**
    - Дані передаються до країн, які забезпечують належний рівень захисту даних відповідно до міжнародних стандартів.
2. **Міжнародні угоди:**
    - Платформа дотримується принципів, викладених у міжнародних угодах, таких як GDPR.
3. **Захисні заходи:**
    - Використовуються стандартні договірні умови або механізми сертифікації для забезпечення безпеки передачі.

5.6. Розкриття даних у разі зміни власника платформи

1. **Права користувачів:**
    - У разі зміни власника платформи користувачі мають право дізнатися, як їхні дані будуть оброблятися надалі.
2. **Передача активів:**
    - Дані користувачів можуть бути передані новому власнику як частина активів платформи.
3. **Нові умови:**
    - Користувачі інформуються про зміну умов обробки даних.

5.7. Політика відносно обробників даних

1. **Контроль над обробниками:**
    - Платформа забезпечує перевірку обробників даних на предмет відповідності нормам захисту даних.
2. **Аудит:**
    - Платформа має право проводити аудит дій обробників даних.
3. **Зобов'язання обробників:**
    - Обробники зобов'язані дотримуватися Політики конфіденційності платформи.

5.8. Обмеження передачі даних

1. **Передача лише за згодою:**
    - Дані можуть бути передані третім сторонам тільки за явною згодою користувача.
2. **Право на заборону передачі:**
    - Користувач має право заборонити передачу своїх даних, крім випадків, передбачених законом.

5.9. Безпека при передачі даних

1. **Шифрування:**
    - Усі дані, що передаються, шифруються з використанням сучасних алгоритмів.
2. **Обмеження доступу:**
    - До переданих даних мають доступ лише уповноважені співробітники третьої сторони.
3. **Технічні заходи:**
    - Використовуються безпечні канали передачі даних (наприклад, HTTPS, VPN).

5.10. Наслідки порушення передачі даних

1. **Відповідальність:**
    - Платформа несе відповідальність за наслідки передачі даних з порушенням умов договору.
2. **Відновлення даних:**
    - У разі порушення безпеки передані дані можуть бути видалені або відновлені у безпечній формі.
3. **Оповіщення:**
    - Користувачі інформуються про будь-які інциденти, пов’язані з передачею їхніх даних.

Розділ 6. Права користувачів

6.1. Право на доступ до своїх даних

Користувач має право отримати доступ до своїх персональних даних, які зберігаються та обробляються платформою.

1. **Запит доступу:**
    - Користувач може подати запит на отримання копії своїх даних через спеціальну форму в налаштуваннях облікового запису або електронною поштою.
2. **Терміни надання:**
    - Платформа зобов'язується надати дані у строк не пізніше 30 днів після отримання запиту.
3. **Форма надання:**
    - Дані надаються в доступному форматі (наприклад, CSV, PDF), який дозволяє легко їх переглядати.
4. **Обсяг інформації:**
    - Надається інформація про категорії зібраних даних, цілі обробки, джерела отримання даних і треті сторони, яким дані були передані.
5. **Обмеження доступу:**
    - Платформа може відмовити у наданні доступу, якщо це суперечить законодавству або може вплинути на права інших осіб.
6. **Повідомлення про відмову:**
    - У разі відмови, користувач отримує письмове пояснення з чіткими причинами.

6.2. Право на виправлення даних

Користувач має право вимагати виправлення неточних або застарілих персональних даних.

1. **Процес виправлення:**
    - Користувач може подати запит на виправлення через налаштування облікового запису або підтримку.

2. **Обґрунтування:**
    - Платформа може вимагати підтвердження правильності нових даних (наприклад, документів).
3. **Терміни виконання:**
    - Виправлення здійснюється протягом 14 днів з моменту подання запиту.
4. **Сповіщення користувача:**
    - Користувач отримує повідомлення про виконання запиту або причини відмови.
5. **Право на обмеження:**
    - У разі суперечливих даних обробка може бути тимчасово обмежена до моменту їх уточнення.
6. **Актуалізація у третіх сторін:**
    - Платформа зобов'язується сповістити треті сторони, яким були передані неправильні дані, про їх виправлення.

6.3. Право на видалення даних

Користувач може вимагати видалення своїх даних у певних випадках.

1. **Умови для видалення:**
    - Дані більше не потрібні для цілей, для яких вони були зібрані.
    - Користувач відкликає згоду на обробку, і немає інших законних підстав для її продовження.
    - Дані були зібрані або оброблені незаконно.
2. **Процедура видалення:**
    - Користувач подає запит через обліковий запис або письмово.
3. **Терміни виконання:**
    - Видалення здійснюється протягом 30 днів після подання запиту.
4. **Обмеження:**
    - Дані не можуть бути видалені, якщо їх обробка необхідна для виконання юридичних зобов’язань або захисту прав інших осіб.

5. **Видалення резервних копій:**
    - Платформа зобов’язується видалити дані з резервних копій у строк, визначений технічними регламентами.

6.4. Право на обмеження обробки

Користувач має право вимагати обмеження обробки своїх даних у певних випадках.

1. **Умови для обмеження:**
    - Дані є неточними, і користувач оскаржує їх правильність.
    - Дані обробляються незаконно, але користувач не хоче їх видалення.
2. **Результат обмеження:**
    - Дані зберігаються, але не використовуються для жодних активних операцій.
3. **Сповіщення:**
    - Користувач отримує підтвердження про застосування обмеження.

6.5. Право на перенесення даних

Користувач має право отримати свої дані у структурованому форматі для передачі іншій платформі.

1. **Формат даних:**
    - Дані надаються у форматах CSV, JSON або XML.
2. **Терміни:**
    - Перенесення здійснюється протягом 30 днів з моменту запиту.
3. **Обмеження:**
    - Перенесення доступне лише для даних, зібраних на основі згоди користувача або договору.

6.6. Право на заперечення обробки

Користувач може заперечити обробку своїх даних з певних причин (наприклад, для маркетингових цілей).

1. **Процедура заперечення:**

- Користувач надсилає письмовий запит або використовує налаштування облікового запису.

2. **Результат:**
   - Платформа припиняє обробку даних, якщо немає вагомих законних підстав для її продовження.

6.7. Право на подання скарги

Користувач має право звернутися до органів захисту даних у разі порушення його прав.

1. **Контактна інформація:**
   - У Політиці конфіденційності надається контакт для звернення до відповідних органів.
2. **Скарга до платформи:**
   - Перед поданням офіційної скарги, користувач може звернутися до служби підтримки.

6.8. Право відкликати згоду

Користувач може відкликати свою згоду на обробку даних у будь-який час.

1. **Процедура відкликання:**
   - Через налаштування облікового запису або письмовий запит.
2. **Результат відкликання:**
   - Платформа припиняє обробку даних, зібраних на основі цієї згоди.

6.9. Зобов'язання платформи щодо реалізації прав

1. **Простота доступу:**
   - Усі процедури повинні бути інтуїтивними та зрозумілими для користувачів.
2. **Відповідність законам:**
   - Платформа забезпечує дотримання всіх норм захисту даних.

Розділ 7. Захист даних

7.1. Технічні заходи захисту даних

Забезпечення безпеки даних через використання сучасних технологій та інструментів.

1. **Шифрування даних:**
    - Всі передані дані (наприклад, через форми реєстрації чи авторизації) шифруються за допомогою протоколів SSL/TLS.
    - Персональні дані, що зберігаються на серверах, захищені алгоритмами AES-256.
2. **Анонімізація:**
    - Для аналітики та звітності використовуються анонімізовані або псевдонімізовані дані.
3. **Системи контролю доступу:**
    - Обмежений доступ до даних для працівників платформи, заснований на принципі "мінімально необхідних привілеїв".
    - Використання двофакторної аутентифікації для доступу до адміністративних систем.
4. **Мережевий захист:**
    - Фаєрволи та системи виявлення вторгнень запобігають несанкціонованому доступу до серверів.
    - Регулярне тестування на наявність вразливостей у програмному забезпеченні.
5. **Резервні копії:**
    - Щоденне створення резервних копій даних із зберіганням їх у захищених місцях.
    - Регулярне тестування процесів відновлення для забезпечення цілісності копій.

7.2. Організаційні заходи захисту даних

Політики та процедури, спрямовані на захист інформації від неправомірного використання.

1. **Політика конфіденційності:**
    - Всі співробітники платформи підписують угоди про нерозголошення інформації (NDA).
2. **Навчання персоналу:**
    - Регулярні тренінги для працівників щодо обробки даних і реагування на кіберзагрози.
3. **Призначення відповідальних осіб:**
    - Призначення Data Protection Officer (DPO), який відповідає за дотримання законодавства щодо конфіденційності.
4. **Журнали доступу:**
    - Ведення детальних журналів дій користувачів і співробітників, які мають доступ до даних.
5. **Оцінка ризиків:**
    - Регулярне проведення аналізу ризиків щодо захисту персональних даних та оновлення політик захисту.

7.3. Захист даних у хмарних сервісах

Платформа використовує хмарні рішення для зберігання та обробки даних.

1. **Вибір постачальників:**
    - Обираються сертифіковані постачальники, які відповідають стандартам ISO 27001, SOC 2 тощо.
2. **Шифрування у хмарі:**
    - Дані шифруються як під час передачі, так і під час зберігання у хмарних сервісах.
3. **Географічне розташування серверів:**
    - Сервери розташовані в країнах, які забезпечують належний рівень захисту даних відповідно до міжнародного законодавства.

7.4. Реагування на інциденти безпеки

Опис дій, які вживаються у разі порушення безпеки даних.

1. **Виявлення інцидентів:**

- Використання автоматизованих систем моніторингу для швидкого виявлення потенційних загроз.

2. **Оцінка впливу:**
   - Проведення аналізу для визначення обсягу та характеру порушення.
3. **Повідомлення користувачів:**
   - Інформування постраждалих користувачів у строк не пізніше 72 годин після виявлення інциденту.
4. **Повідомлення регуляторів:**
   - Сповіщення відповідних органів, якщо порушення даних може вплинути на значну кількість користувачів.
5. **Мінімізація наслідків:**
   - Вжиття заходів для обмеження впливу інциденту, включаючи блокування доступу до системи.

7.5. Технічні аудитори безпеки

Залучення зовнішніх спеціалістів для оцінки системи захисту.

1. **Періодичні перевірки:**
   - Аудити проводяться щонайменше раз на рік.
2. **Підготовка звітів:**
   - Висновки аудиторів документуються та використовуються для вдосконалення системи захисту.

7.6. Реагування на витік даних

Алгоритм дій, якщо дані користувачів опиняться у відкритому доступі.

1. **Ідентифікація джерела витоку:**
   - Визначення причини та локалізація проблеми.
2. **План дій:**
   - Негайне впровадження заходів щодо припинення витоку даних.
3. **Інформування користувачів:**
   - Надання рекомендацій для мінімізації ризиків, таких як зміна паролів.

7.7. Відповідальність користувачів за безпеку даних

1. **Сильні паролі:**
    - Рекомендація використовувати паролі, що містять не менше 12 символів, великі та малі літери, цифри і спеціальні символи.
2. **Регулярна зміна паролів:**
    - Користувачам пропонується змінювати паролі щонайменше раз на 6 місяців.

7.8. Захист даних під час передачі

1. **Канали передачі:**
    - Дані передаються лише через захищені канали HTTPS.
2. **Міжнародна передача:**
    - Дані передаються між країнами лише за наявності відповідних юридичних угод.

7.9. Відновлення систем після аварій

1. **Резервні системи:**
    - Наявність дублюючих серверів для забезпечення роботи платформи у разі збоїв.
2. **Тестування процедур:**
    - Регулярні навчальні вправи для відпрацювання відновлення після аварій.

7.10. Регулярне оновлення політик захисту

1. **Оновлення безпеки:**
    - Адаптація до нових технологій захисту.
2. **Повідомлення користувачів:**
    - Інформування про зміни, що впливають на захист даних.