Політика конфіденційності та DPA Zapys24

Ця Політика описує, як Компанія збирає, використовує, зберігає та захищає персональні дані користувачів і їхніх клієнтів, а також визначає взаємини між Контролером (Користувачем) та Процесором (Компанією) згідно із законодавством України та положеннями GDPR.

2.1 Хто відповідає за обробку

• Контролер: Користувач (юридична чи фізична особа), який завантажує або обробляє персональні дані клієнтів через Zapys24.

• Процесор: ФОП «Zapys24», що надає технічні засоби для обробки даних.

• Контактні дані Компанії для питань конфіденційності: [електронна адреса].

• Якщо у вас призначений офіцер із захисту даних (DPO), зазначте його контактні дані.

2.2 Правові підстави та мета обробки

1. Правові підстави. Ми обробляємо персональні дані на підставі:

• згоди суб’єкта даних;

• виконання договору (надання сервісу);

• легітимного інтересу (наприклад, забезпечення безпеки та запобігання шахрайству);

• дотримання правових зобов’язань.

1. Цілі обробки.

• реєстрація та управління аккаунтами користувачів;

• надання доступу до функціоналу сервісу;

• обробка платежів (через інтегрованих платіжних провайдерів);

• надсилання сервісних повідомлень і сповіщень;

• аналітика використання для покращення сервісу;

• підтримка та обробка запитів.

1. Автоматизоване прийняття рішень. Ми не використовуємо автоматизоване прийняття рішень, яке має юридичні наслідки для суб’єктів даних (наприклад, кредитні скоринги). Якщо такі механізми з’являться, ми окремо повідомимо користувачів та забезпечимо можливість оскаржити рішення.

2.3 Типи та категорії даних

Ми можемо збирати такі категорії даних:

• Ідентифікаційні дані: ім’я, прізвище, назва компанії, ІПН, логін, пароль, ID користувача;

• Контактні дані: email, номер телефону, адреса (за потреби);

• Платіжні дані: номер рахунку, транзакційні ідентифікатори (обробляються платіжними провайдерами, ми не зберігаємо повні реквізити карт);

• Дані клієнтів користувача: контактні та фінансові дані ваших клієнтів, які ви завантажуєте в систему;

• Файли та документи: завантажені зображення чи документи, пов’язані з клієнтами;

• Технічні дані: IP-адреса, тип пристрою, дані про браузер, файли cookie та журнал дій;

• Логи обробки: історія доступу до записів, операції з даними.

2.4 Джерела та способи збору

• Дані, які ви надаєте самостійно під час реєстрації чи користування сервісом.

• Дані, що отримуються автоматично через файли cookie та аналітичні інструменти (див. Політику щодо cookie).

• Дані, які ми отримуємо від платіжних провайдерів про статус платежів (без доступу до платіжних реквізитів).

2.5 Передача та розкриття даних третім сторонам

1. Платіжні провайдери. Дані про оплати передаються платіжним системам (наприклад, monobank) для обробки транзакцій. Вони виступають окремими контролерами.

2. Постачальники хостингу та IT-інфраструктури. Дані зберігаються на серверах хостинг-провайдерів (може бути у межах України чи ЄС). Ми укладаємо договори (DPA) з провайдерами щодо належного захисту даних.

3. Аналітичні та маркетингові інструменти. Використовуються лише за наявності згоди користувача; перелік і призначення кожного з таких постачальників буде опубліковано в окремому додатку до цієї політики.

4. Державні органи. Ми можемо передавати дані у випадках, коли це вимагається законом або рішенням суду.

2.6 Міжнародні передачі

Якщо дані передаються за межі України, ми забезпечуємо, щоб отримувач дотримувався адекватного рівня захисту (наприклад, відповідно до статті 45 GDPR або стандартних договірних положень).

2.7 Тривалість зберігання

Ми зберігаємо персональні дані лише протягом часу, необхідного для досягнення цілей обробки, або відповідно до вимог законодавства. Критерії визначення термінів:

• Термін дії підписки та 30 днів після її завершення;

• Період вимог законодавства щодо бухгалтерського обліку;

• До відкликання згоди (для маркетингових розсилок);

• Для даних у резервних копіях — до циклу їх видалення (до 90 днів).

2.8 Права суб’єктів даних

Користувачі та їхні клієнти мають наступні права:

• Право бути поінформованим про способи використання своїх даних;

• Право доступу до своїх персональних даних;

• Право на виправлення неточних або неповних даних;

• Право на видалення («право на забуття»);

• Право на обмеження обробки;

• Право на переносимість даних (отримання копії у структурованому форматі);

• Право заперечити проти обробки на підставі легітимного інтересу;

• Право подати скаргу до наглядового органу;

• Право відкликати згоду у будь-який момент (це не впливає на законність обробки до відкликання).

Щоб реалізувати права, слід звернутися через контактні дані, зазначені вище. Ми маємо право перевірити вашу особу перед виконанням запиту.

2.9 Безпека та технічні заходи

Ми впроваджуємо технічні та організаційні заходи для захисту даних:

• шифрування даних при передаванні та зберіганні;

• автентифікація та контроль доступу, журнали доступу;

• регулярне тестування та оновлення безпеки;

• резервне копіювання та відновлення даних;

• політики управління паролями та двофакторна автентифікація;

• моніторинг інцидентів та процедура повідомлення про порушення безпеки;

• навчання персоналу щодо конфіденційності та захисту даних.

2.10 Угода про обробку даних (DPA)

Оскільки ви (Користувач) виступаєте Контролером, а ми (Компанія) — Процесором, ми укладаємо DPA, що регламентує:

1. Предмет і обсяг обробки. Визначає, що Компанія обробляє персональні дані клієнтів користувача лише для надання послуг, не використовуючи їх для власних цілей.

2. Термін дії та розірвання. DPA діє протягом строку користування сервісом; після розірвання ми видаляємо або повертаємо всі персональні дані та копії.

3. Обов’язки контролера. Користувач відповідає за законність збору даних, надання інструкцій щодо їх обробки, опрацювання запитів суб’єктів даних та за забезпечення, що дані не містять спеціальних категорій без відповідних підстав.

4. Обов’язки процесора. Компанія зобов’язується:

• забезпечити належні технічні та організаційні заходи захисту;

• обробляти дані виключно за інструкціями контролера;

• не залучати суб-процесорів без письмової згоди контролера;

• повідомляти про інциденти безпеки та співпрацювати з наглядовими органами;

• допомагати у виконанні прав суб’єктів даних;

• вести записи про обробку даних та надавати їх для аудиту.

1. Суб-процесори. Ми можемо залучати суб-процесорів (наприклад, хостинг-провайдерів) за умови, що вони надають достатні гарантії щодо захисту даних. Перелік суб-процесорів міститься в Додатку 2 до DPA.

2. Технічні та організаційні заходи. Докладний опис заходів безпеки наведений у Додатку 1 до DPA (конфіденційність, цілісність, доступність та процедури періодичного перегляду).

3. Фінальні положення. Зміни до DPA можливі лише за згодою обох сторін; DPA має пріоритет над іншими угодами між сторонами.

2.11 Зміни політики

Ми можемо час від часу оновлювати цю Політику. В такому випадку ми повідомимо про це, змінивши дату оновлення й, за необхідності, через електронні повідомлення. Рекомендуємо регулярно переглядати Політику для ознайомлення з актуальними умовами.

2.12 Обробка даних дітей

1. Вік та згода батьків. Ми дотримуємося вимог GDPR щодо захисту дітей. Якщо ви обробляєте дані осіб молодше мінімального віку для надання згоди (13–16 років, залежно від юрисдикції), ви повинні отримати підтвердження згоди законного представника.

2. Заборона маркетингу дітям. Дані дітей використовуються виключно для надання сервісу й не застосовуються в маркетингових цілях без явної згоди батьків.

3. Право на видалення. Батьки або законні представники можуть вимагати видалення персональних даних дітей у будь-який момент, і ми будемо діяти без невиправданої затримки.

4. Простота мови. Повідомлення, адресовані дітям, мають бути зрозумілими та написані простою мовою, відповідно до рекомендацій Європейської комісії.

2.13 Маркетингові комунікації

1. Окрема згода. Ми надсилаємо маркетингові та промоційні повідомлення лише за наявності окремої добровільної згоди. Ви можете відкликати її у будь-який час, і ми негайно припинимо розсилки.

2. Правові підстави. Для відправлення сервісних повідомлень ми спираємося на виконання договору; для маркетингових — на згоду або наш легітимний інтерес, якщо це дозволено законом.

3. Відписка. Кожне маркетингове повідомлення міститиме інструкції для відписки або зміни налаштувань комунікацій.

2.14 Анонімізація та псевдонімізація

1. Псевдонімізація. У процесі обробки ми можемо замінювати ідентифікаційні дані унікальними ідентифікаторами, що знижує ризик ідентифікації та допомагає нам

виконувати вимоги безпеки.

2. Анонімізація. Для аналітики ми можемо використовувати агреговані та повністю анонімізовані дані, які не дозволяють ідентифікувати осіб навіть у комбінації з іншими наборами даних.

3. Обмеження. Псевдонімізовані дані залишаються персональними даними, тому ми застосовуємо ті самі високі стандарти захисту та доступу.

2.15 Повідомлення про порушення та інциденти

1. 72-годинне правило. У випадку порушення безпеки, яке створює ризики для прав та свобод суб’єктів даних, ми повідомляємо компетентний наглядовий орган протягом 72 годин з моменту виявлення.

2. Інформування користувачів. Якщо порушення може спричинити високий ризик для користувачів, ми повідомимо їх, описавши характер інциденту, можливі наслідки та заходи захисту.

3. Журнали інцидентів. Ми ведемо журнал інцидентів і співпрацюємо із контролюючими органами та контролерами у процесі розслідування.

2.16 Оцінка впливу на захист даних (DPIA)

1. Коли проводиться. Якщо плануються нові операції з високим ризиком (наприклад, використання біометричних даних або системи оцінки), ми проводимо оцінку впливу на захист даних (Data Protection Impact Assessment).

2. Участь контролера. Ми співпрацюємо з контролером у проведенні DPIA, надаємо необхідну інформацію та реалізуємо запропоновані заходи пом’якшення ризиків.

3. Результати. Результати DPIA можуть включати додаткові технічні або організаційні заходи, які ми впроваджуємо перед запуском відповідної обробки.

2.17 Представництво в ЄС та міжнародні трансфери

1. Представник у ЄС. Якщо наша діяльність підпадає під вимоги GDPR, ми призначимо представника в ЄС для взаємодії з наглядовими органами та суб’єктами даних.

2. Адекватність та договори. При передачі даних за межі Європейської економічної зони ми використовуємо механізми з належним рівнем захисту — стандартні договірні положення або рішення про адекватність від Європейської комісії.

3. Локальні вимоги. Користувачі несуть відповідальність за дотримання місцевих вимог щодо міжнародних трансферів даних.

2.18 Зміни та доповнення до DPA

1. Процедура зміни. Усі зміни до DPA мають бути узгоджені сторонами. Ми повідомимо користувачів про пропоновані зміни та надамо можливість висловити заперечення.

2. Пріоритет. У разі конфлікту між DPA та іншими угодами пріоритет матиме DPA, якщо інше не передбачено законом.

3. Архівування. Ми зберігаємо історію змін DPA для забезпечення прозорості та доказів виконання.

2.19 Контроль доступу та навчання персоналу

1. Принцип мінімального доступу. Доступ до персональних даних надається лише тим працівникам і підрядникам, які потребують цього для виконання своїх посадових обов’язків. Доступ переглядається регулярно та одразу відкликається при завершенні співпраці.

2. Навчання. Всі співробітники проходять регулярне навчання щодо конфіденційності та інформаційної безпеки, у тому числі правил поводження з персональними даними та реагування на інциденти.

3. Відстеження доступу. Ведеться журнал доступу до даних, щоб можна було простежити, хто, коли та з якою метою отримував доступ.

2.20 Відповідальність за субпідрядників

1. Контроль суб-процесорів. Ми гарантуємо, що всі суб-процесори, залучені до обробки даних, надають такі самі рівні захисту, як і ми. Вони підписують угоди про обробку даних та виконують свої зобов’язання.

2. Перелік суб-процесорів. Актуальний список суб-процесорів зберігається в додатку до цієї Політики. Користувач буде повідомлений про зміни заздалегідь.

3. Збереження відповідальності. Попри залучення суб-процесорів, ми залишаємося відповідальними за дотримання умов DPA та належний захист даних.

2.21 Процедура подання скарг та звернення

1. Внутрішні звернення. Якщо у вас є скарги чи запитання щодо обробки персональних даних, зв’яжіться з нами через контакти, зазначені у цій Політиці. Ми розглянемо запит і надамо відповідь протягом 30 днів.

2. Наглядові органи. Суб’єкти даних можуть подати скаргу до місцевого наглядового органу з питань захисту даних, якщо вони вважають, що їхні права були порушені.

3. Позасудове врегулювання. Ми заохочуємо вирішувати питання шляхом переговорів та медіації перед зверненням до суду чи регуляторів.