MedSales Academy

https://medsales-academy.sendpulse.courses

Зареєстровано в Республіці Польща

ПОЛІТИКА ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

Внутрішній нормативний документ · Відповідає GDPR та законодавству Республіки Польща

Документ розроблено відповідно до: Регламенту (ЄС) 2016/679 (GDPR); Закону Польщі від 10.05.2018 р. про захист персональних даних (Dz.U. 2018 poz. 1000); Закону від 18.07.2002 р. про надання послуг електронними засобами; Закону від 16.07.2004 р. «Про телекомунікації» (в частині cookie). Контрольний орган: UODO (Urząd Ochrony Danych Osobowych).

1. Загальні положення та правова база

1.1. Ця Політика обробки персональних даних (далі — «Політика») є внутрішнім нормативним документом IHOR HRYTSENKO (далі — «Адміністратор»), зареєстрованої в Республіці Польща, що здійснює освітню діяльність у рамках проєкту MedSales Academy.

1.2. Метою Політики є визначення принципів, процедур та інструментів, що забезпечують обробку персональних даних відповідно до GDPR та пов'язаного польського законодавства.

1.3. Дія Політики поширюється на:

— всіх співробітників та осіб, що діють від імені Адміністратора та мають доступ до персональних даних;

— всіх обробників, із якими Адміністратором укладено DPA (угоду про обробку даних, ст. 28 GDPR);

— всі операції з обробки персональних даних клієнтів, потенційних клієнтів і партнерів.

1.4. Адміністратор призначає відповідальну особу за захист даних (DPO — якщо застосовується ст. 37 GDPR) або особу, відповідальну за виконання зобов'язань у сфері захисту даних.

2. Реєстр операцій з обробки (RoPA — ст. 30 GDPR)

2.1. Адміністратор веде письмовий реєстр усіх операцій з обробки персональних даних (Record of Processing Activities) відповідно до ст. 30 GDPR, що містить:

1. найменування та контактні дані Адміністратора та, за наявності, DPO;

2. цілі обробки;

3. категорії суб'єктів даних та категорії персональних даних;

4. категорії одержувачів, яким персональні дані розкривалися або розкриватимуться;

5. інформацію про передачу до третіх країн та застосовані гарантії;
6. передбачені строки видалення даних;
7. опис технічних та організаційних заходів безпеки (ст. 32 GDPR).

2.2. RoPA оновлюється при будь-яких змінах в операціях обробки та надається на вимогу UODO.

3. Категорії персональних даних та суб'єктів

База даних	Категорії суб'єктів	Категорії даних
Клієнти та користувачі	Фізичні особи — покупці курсу	Ім'я, прізвище, e-mail, телефон, платіжні дані, прогрес навчання, IP
Потенційні клієнти	Особи, що залишили заявку	Ім'я, e-mail, телефон, зміст запиту
Співробітники	Персонал Адміністратора	Відповідно до трудового законодавства PL (окреме положення)
Маркетинг (за згодою)	Підписники розсилки	E-mail, ім'я, дата/спосіб надання згоди

3.1. Адміністратор НЕ обробляє спеціальні категорії даних (ст. 9 GDPR) без явної та окремої згоди суб'єкта або за відсутності інших підстав, передбачених ст. 9(2) GDPR.

3.2. Персональні дані дітей до 16 років (відповідно до ст. 8 GDPR та ст. 5 польського Закону від 10.05.2018 р.) можуть оброблятися лише за наявності згоди батьків або законних представників. Послуги MedSales Academy призначені виключно для осіб, що досягли 18 років.

4. Принципи обробки персональних даних (ст. 5 GDPR)

4.1. Усі операції з обробки персональних даних здійснюються відповідно до таких принципів:

1. Законність, справедливість, прозорість (ст. 5(1)(a)) — обробка лише на законних підставах і у спосіб, зрозумілий суб'єкту даних.
2. Обмеження мети (ст. 5(1)(b)) — збір виключно для конкретних, явних і законних цілей; забороняється подальша обробка, несумісна з початковою метою.
3. Мінімізація даних (ст. 5(1)(c)) — обробляються лише дані, що є адекватними, доречними та необхідними.
4. Точність (ст. 5(1)(d)) — дані підтримуються актуальними; неточні — виправляються або видаляються без зволікань.
5. Обмеження строку зберігання (ст. 5(1)(e)) — дані зберігаються у формі, що уможливлює ідентифікацію, не довше, ніж необхідно для цілей обробки.
6. Цілісність і конфіденційність (ст. 5(1)(f)) — захист від несанкціонованої обробки, втрати або пошкодження.
7. Підзвітність (ст. 5(2)) — Адміністратор здатний продемонструвати дотримання всіх принципів.

5. Правові підстави обробки (ст. 6 GDPR) — деталізація

5.1. Обробка на підставі згоди (ст. 6(1)(a) GDPR):

— Згода отримується у формі явної активної дії (opt-in): прапорець у формі реєстрації, підтвердження в email.

— Кожна ціль — окрема згода (маркетинг не поєднується із сервісними умовами).

— Адміністратор документує: ким, коли, у який спосіб і для якої мети надано згоду.

— Відкликання здійснюється: через налаштування акаунта, посилання у листі, email-запит. Відкликання не впливає на правомірність обробки до відкликання.

5.2. Обробка для виконання договору (ст. 6(1)(b) GDPR):

— Підставою є договір з суб'єктом або заходи на запит суб'єкта перед укладенням договору.

— Надання даних є необхідною умовою отримання послуги; без них виконання договору неможливе.

5.3. Обробка для виконання правового обов'язку (ст. 6(1)(c) GDPR):

— Ведення фінансової документації (Закон Польщі від 29.09.1994 р. про бухгалтерський облік).

— Виконання вимог податкового законодавства (Закон про ПДВ, Закон про податок на прибуток).

— Надання даних уповноваженим органам на законних підставах.

5.4. Обробка на підставі законного інтересу (ст. 6(1)(f) GDPR):

— Захист Адміністратора від шахрайства та порушень умов користування.

— Аналітика та покращення якості послуг (знеособлена статистика).

— Захист прав у судових та позасудових спорах.

— Адміністратор проводить задокументований тест балансу інтересів для кожної мети на цій підставі.

6. Управління згодами та їх відкликання

6.1. Вимоги до дійсної згоди (ст. 7 GDPR):

— Вільна — не може обумовлюватися наданням послуги (крім випадків, коли обробка необхідна для її виконання).

— Конкретна — для кожної мети окремо.

— Поінформована — чіткий опис мети, категорій даних, права на відкликання.

— Однозначна — виражена через активну дію (не попередньо встановлені прапорці, не мовчання).

6.2. Адміністратор веде реєстр наданих/відкликаних згод із зазначенням: ID суб'єкта, дати та способу надання, точного тексту, що відображався, та дати відкликання (за наявності).

6.3. Згода на маркетингові комунікації підтверджується механізмом double opt-in (e-mail підтвердження підписки).

6.4. Суб'єкт може відкликати будь-яку згоду в будь-який час без негативних наслідків для доступу до послуг, що не залежать від такої згоди.

7. Строки зберігання персональних даних

Категорія даних	Строк зберігання	Правова підстава
Договірні дані клієнтів	5 років від закінчення договору	ст. 6(1)(b)(c) GDPR + Закон про бухоблік PL
Платіжні та фіскальні документи	5 років з кінця фінансового року	Податкове законодавство PL
Маркетингові згоди	До відкликання + 3 роки для доказів	ст. 6(1)(a) GDPR
Технічні логи / безпека	12 місяців	ст. 6(1)(f) GDPR
Запити підтримки	2 роки після закриття	ст. 6(1)(f) GDPR
Неактивні акаунти	3 роки від останньої активності	ст. 6(1)(f) GDPR
Аналітичні cookie	13 місяців	Рекомендації UODO / CNIL
Дані про порушення безпеки	5 років (документація)	ст. 33(5) GDPR

7.1. Після закінчення строку зберігання персональні дані знищуються надійним способом або знеособлюються. Процедура знищення документується.

8. Оцінка впливу на захист даних (DPIA — ст. 35 GDPR)

8.1. Адміністратор проводить DPIA перед початком операцій з обробки, що можуть становити високий ризик для прав і свобод фізичних осіб, зокрема:

— систематичного і масштабного профілювання;

— обробки спеціальних категорій даних у великому масштабі;

— систематичного моніторингу загальнодоступних місць у великому масштабі.

8.2. Якщо DPIA свідчить про залишковий високий ризик, Адміністратор звертається до UODO за попередньою консультацією (ст. 36 GDPR).

9. Обробники та треті сторони (ст. 28–29 GDPR)

9.1. Перед залученням обробника Адміністратор проводить перевірку:

— наявності технічних і організаційних заходів, що відповідають GDPR;

— дотримання принципів захисту даних та підзвітності;

— юрисдикції та відповідних механізмів для передачі до третіх країн.

9.2. З кожним обробником укладається DPA (угода про обробку даних), що містить обов'язкові елементи ст. 28(3) GDPR: предмет, строк, характер і мету обробки, тип даних, категорії суб'єктів, права та зобов'язання сторін.

9.3. Обробник може залучати субобробників лише з попереднього письмового дозволу Адміністратора. Адміністратор веде актуальний перелік обробників та субобробників.

9.4. Субобробники зобов'язані відповідати тим самим вимогам захисту даних, що й основний обробник.

10. Технічні та організаційні заходи захисту (ст. 32 GDPR)

10.1. Технічні заходи (з урахуванням «стану мистецтва» відповідно до ст. 32(1)):

— Шифрування при передачі (TLS 1.2+) та у стані спокою (AES-256 або аналог).

— Псевдонімізація персональних даних (де технічно застосовується).

— Резервне копіювання з перевіркою відновлення.

— Журналювання доступу до персональних даних.

— Управління вразливостями та регулярне оновлення ПЗ.

— Багатофакторна автентифікація для адміністративних систем.

10.2. Організаційні заходи:

— Призначення відповідальних осіб за різні категорії обробки.

— Регулярне навчання персоналу (не рідше 1 разу на рік) з питань GDPR і кібербезпеки.

— Чіткі внутрішні процедури обробки запитів суб'єктів даних.

— Процедура реагування на порушення безпеки з чек-листом та строками.

— Перевірка третіх сторін (due diligence) перед укладенням DPA.

— Регулярний внутрішній аудит відповідності GDPR (не рідше 1 разу на рік).

11. Процедура реагування на порушення безпеки (ст. 33–34 GDPR)

11.1. При виявленні або підозрі на порушення захисту персональних даних відповідальна особа зобов'язана:

1. Негайно зафіксувати факт виявлення з точним часом.

2. Провести первинну оцінку ризику для прав і свобод суб'єктів даних протягом 1 (однієї) години.

3. Якщо ризик не є незначним — повідомити UODO протягом 72 (сімдесяти двох) годин від виявлення (ст. 33(1) GDPR). Якщо повідомлення затримується — вказати причини.

4. Якщо ризик є «високим» — без зайвої затримки повідомити безпосередньо постраждалих суб'єктів (ст. 34 GDPR).

5. Документувати інцидент у реєстрі порушень з: описом порушення, категоріями та кількістю постраждалих суб'єктів, можливими наслідками, вжитими заходами.

6. Провести пост-інцидентний аналіз та впровадити превентивні заходи.

11.2. Повідомлення до UODO (ст. 33(3) GDPR) містить: характер порушення, категорії та приблизну кількість постраждалих, контактні дані DPO, ймовірні наслідки, вжиті або заплановані заходи.

12. Права суб'єктів та внутрішня процедура їх реалізації

12.1. Запит суб'єкта може надійти в будь-якій формі (e-mail, пошта, усно). Відповідальна особа реєструє запит негайно після отримання.

12.2. Строки відповіді: 1 (один) місяць з дати отримання запиту. За складних запитів — продовження на 2 (два) місяці з повідомленням протягом першого місяця.

12.3. Верифікація особи суб'єкта здійснюється засобами, пропорційними ризику помилкової ідентифікації (не допускаючи надмірного збору додаткових даних).

12.4. Якщо запит є явно безпідставним або надмірним (напр., повторюваним), Адміністратор може відмовити у виконанні або стягнути обґрунтований збір, документуючи рішення.

12.5. Реєстр запитів суб'єктів зберігається для демонстрації підзвітності (ст. 5(2) GDPR).

13. Навчання та підвищення обізнаності

13.1. Всі особи, що мають доступ до персональних даних, проходять обов'язковий вступний інструктаж з GDPR перед початком обробки та щорічне повторне навчання.

13.2. Програма навчання охоплює: принципи GDPR, правові підстави, права суб'єктів, процедуру реагування на порушення, практику безпечної обробки.

13.3. Факт проходження навчання документується.

14. Зміни до Політики та перегляд

14.1. Ця Політика переглядається не рідше одного разу на рік, а також при: суттєвих змінах у законодавстві або рекомендаціях UODO; введенні нових операцій обробки; виявлених порушеннях або результатах аудиту.

14.2. Усі версії Політики архівуються протягом не менше 5 (п'яти) років.

15. Контактна інформація

Адміністратор: IHOR HRYTSENKO

Адреса: Region Śląskie, Gliwice ul. Czwartaków 11/27, Poland

NIP: 6312731797 / REGON: Śląskie

E-mail: medsales.academyonline@gmail.com

Ця Політика затверджена Адміністратором та набирає чинності з дати підписання.