Товариство з обмеженою відповідальністю “Маркет Віжн”
Код ЄДРПОУ: 44000963. Адреса: 03150 Україна, м. Київ, вул. Велика Васильківська, 114
Тел.: +38 (096) 388 9966. Веб-сайт: research.ua, e-mail: info@research.ua

ЗАТВЕРДЖЕНО

Директор ТОВ «Маркет Віжн»

_____ Ніна Делюкова

(підпис)

«01» січня 2026 р.

ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ЗАХИСТУ ДАНИХ

ТОВ «Маркет Віжн» (Research.ua)

м. Київ – 2026

Зміст

1. Сфера застосування
2. Нормативні документи
3. Терміни та визначення
4. Політика інформаційної безпеки
5. Класифікація інформації та управління доступом
6. Отримання згоди на обробку персональних даних
7. Управління базами даних, які містять персональні дані
8. Дії у випадку виявлення витоку персональних даних
9. Надання інформації та персональних даних третім особам
10. Відповідальність

1. СФЕРА ЗАСТОСУВАННЯ

Ця політика визначає вимоги щодо захисту інформації від несанкціонованого доступу та захисту персональних даних у ТОВ «Маркет Віжн» (надалі Research.ua), яке працює під торговою маркою Research.ua.

Вимоги політики поширюються на:

- усіх штатних співробітників ТОВ «Маркет Віжн»;
- пов'язаних організацій та структур, що діють під торговою маркою Research.ua;
- ФОП-партнерів та зовнішніх підрядників, що залучаються до проєктів Research.ua;
- будь-яких третіх осіб, що отримують доступ до інформаційних систем або даних компанії.

Політика охоплює всі інформаційні активи Research.ua: дані в Google Workspace (Drive, Gmail, Meet), survey-платформах, панельних системах (Власна Думка, Senso), аналітичні файли (SPSS, Excel), а також будь-яку паперову документацію.

2. НОРМАТИВНІ ДОКУМЕНТИ

Ця політика розроблена відповідно до:

- Закону України «Про інформацію»;
- Закону України «Про захист персональних даних» (№ 2297-VI від 01.06.2010);
- Регламенту (ЄС) 2016/679 (GDPR) — у частині, що стосується персональних даних суб'єктів з країн ЄС.

3. ТЕРМІНИ ТА ВИЗНАЧЕННЯ

інформація – будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді;

персональні дані – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована;

база персональних даних – іменована сукупність упорядкованих персональних даних в електронній формі та/або у формі картотек;

володілець персональних даних – юридична особа (ТОВ «Рісерч.юей»), що визначає мету обробки персональних даних;

розпорядник персональних даних – особа, якій надано право обробляти персональні дані від імені володільця;

суб'єкт персональних даних – фізична особа, персональні дані якої обробляються (респондент, співробітник, партнер, учасник дослідження);

інцидент ІБ – подія, що реально або потенційно порушує конфіденційність, цілісність або доступність інформаційних активів компанії;

конфіденційна інформація – дані клієнтів, донорів, результати досліджень, комерційні пропозиції та внутрішні документи, що не підлягають розголошенню.

4. ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Політика інформаційної безпеки Research.ua визначає основні принципи, напрямки та вимоги щодо захисту інформації компанії, її співробітників, клієнтів, донорів та респондентів.

Обробка інформації та персональних даних у Research.ua здійснюється відповідно до вимог законодавства України та міжнародних стандартів. Інформаційна безпека постійно вдосконалюється шляхом виконання вимог цієї політики усіма співробітниками та партнерами, виділення ресурсів на заходи з підвищення захищеності та регулярного перегляду процедур.

Завданнями системи інформаційної безпеки Research.ua є:

- дотримання вимог законодавства України та міжнародних стандартів;
- класифікація інформації за рівнями конфіденційності та забезпечення відповідних прав доступу;
- захист персональних даних респондентів, клієнтів, донорів та співробітників;
- управління ризиками, пов'язаними з інформаційною безпекою (MV-PROC-RM-001);
- забезпечення безперервності основних бізнес-процесів та мінімізація шкоди від інцидентів ІБ;
- розробка та підтримка процедур реагування на інциденти (MV-PROC-ERP-001);
- навчання персоналу та партнерів з питань інформаційної безпеки.

Обов'язкові технічні вимоги до кожного співробітника та партнера Research.ua:

- двофакторна аутентифікація (2FA) для всіх корпоративних облікових записів Google Workspace;
- унікальний надійний пароль для корпоративного облікового запису;
- антивірусний захист на робочому пристрої;
- передача конфіденційних файлів виключно через захищені посилання Google Drive;
- зберігання конфіденційних файлів виключно на корпоративному Google Drive (не на особистих акаунтах або пристроях без резервної копії).

5. КЛАСИФІКАЦІЯ ІНФОРМАЦІЇ ТА УПРАВЛІННЯ ДОСТУПОМ

Уся інформація Research.ua класифікується за чотирма рівнями:

Рівень	Приклади	Правила доступу
Суворо конфіденційна	Масиви даних з іменами/телефонами респондентів; паролі; фінансові умови договорів	Лише визначені особи. Передача – виключно захищеними каналами.
Конфіденційна	Звіти до публікації; КП; методологія; дані клієнтів і донорів	Команда проєкту + керівництво. Не передається зовнішнім особам без NDA.
Внутрішня	Внутрішні інструкції, шаблони, комунікації команди	Всі співробітники та залучені партнери.
Публічна	Публікації на сайті research.ua, прес-релізи	Без обмежень.

Доступ до інформаційних систем надається за принципом мінімальних привілеїв – лише в обсязі, необхідному для виконання конкретних функцій. Права доступу призначаються СОО або адміністратором Google Workspace. Після завершення співпраці з партнером або підрядником – доступ відкликається протягом 2 робочих днів.

6. ОТРИМАННЯ ЗГОДИ НА ОБРОБКУ ПЕРСОНАЛЬНИХ ДАНИХ

Згоду на обробку персональних даних Research.ua отримує від: респондентів (учасників досліджень), співробітників та ФОП-партнерів.

Відповідно до Закону України «Про захист персональних даних» (№ 2297-VI від 01.06.2010), обробка персональних даних допускається лише за згодою особи або на іншій законній підставі.

Персональні дані, що обробляються Research.ua в рамках дослідницьких проєктів, включають:

- основні ідентифікаційні дані: ПІБ, дата народження, ідентифікаційний номер (за необхідності);
- контактні дані: адреса, номер телефону, email;
- соціально-демографічні характеристики: стать, вік, освіта, місце проживання, зайнятість;
- відповіді в анкетах та дані інтерв'ю, фокус-груп, UX-сесій.

Особливі категорії персональних даних (стан здоров'я, політичні чи релігійні переконання, расове або етнічне походження) обробляються Research.ua виключно за явною письмовою згодою суб'єкта та лише в обсязі, необхідному для конкретного дослідження.

Форма згоди на обробку персональних даних (Додаток 1 до цієї процедури) містить:

- найменування особи (компанії), що здійснює обробку даних;
- перелік персональних даних, що підлягають обробці;
- конкретну мету обробки;
- спосіб обробки та передачі даних третім особам (за наявності);
- права суб'єкта даних, у тому числі право на відкликання згоди;
- строк дії згоди або умови її припинення.

Згода має бути добровільною, конкретною та вираженою чіткою дією (підпис, галочка у незаповненому полі). «Мовчазна» згода або автоматичне погодження через умови користування не допускаються.

Суб'єкт персональних даних має право відкликати свою згоду в будь-який час. Research.ua зобов'язана припинити обробку таких даних, якщо немає іншої законної підстави.

7. УПРАВЛІННЯ БАЗАМИ ДАНИХ, ЯКІ МІСТЯТЬ ПЕРСОНАЛЬНІ ДАНІ

Усі персональні дані, що обробляються у Research.ua, зберігаються у захищених базах даних. Перелік баз даних наведено у Таблиці 1 – Картотека баз даних, які містять персональні дані.

Відповідальна особа реєструє кожну нову базу даних у картотеці. Зберігання персональних даних передбачає забезпечення їх цілісності та відповідного режиму доступу згідно з вимогами Закону України «Про захист персональних даних».

Таблиця 1. Реєстр баз даних, які містять персональні дані

№	Назва бази даних	Вид персональних даних	Розміщення	Тип інформації	Відповідальна особа	Дата початку ведення
1	База респондентів панелі Власна Думка	Контактні дані, соціально-демографічні характеристики	Сервер панелі / Google Drive	Електронна	Head of Fieldwork	
2	База респондентів панелі Senso	Контактні дані, соціально-демографічні	Сервер панелі / Google Drive	Електронна	Head of Fieldwork	

		характеристики				
3	Особові дані співробітників	ПІБ, ІПН, паспортні дані, контакти	Google Drive (захищена папка HR)	Електронна	HR Manager	
4	Договори ФОП-партнерів	ПІБ, ІПН, реквізити	Google Drive / 1С	Електронна	Finance Manager	
5	Масиви даних досліджень (з персональними даними)	Контактні дані, відповіді респондентів	Google Drive (захищена папка проєкту)	Електронна	PM / Head of Fieldwork	
6	Дані учасників якісних досліджень	ПІБ, контакти, записи сесій	Google Drive (захищена папка проєкту)	Електронна / аудіо/відео	PM / Head of Research	
7	Резюме кандидатів	ПІБ, контакти, досвід роботи	Google Drive (HR)	Електронна	HR Manager	

У разі формування нової бази даних, що містить персональні дані, відповідальна особа вносить її до реєстру протягом 5 робочих днів.

Терміни зберігання персональних даних:

- контактні дані респондентів – до 12 місяців після завершення проєкту або відповідно до умов договору;
- знеособлені масиви відповідей – 5 років або відповідно до вимог донора;
- аудіо/відео записи сесій – до затвердження транскрипту клієнтом, але не більше 6 місяців;
- особові дані співробітників – протягом дії трудових відносин + 3 роки;
- дані ФОП-партнерів – протягом дії договірних відносин + 3 роки.

8. ДІЇ У ВИПАДКУ ВИЯВЛЕННЯ ВИТОКУ ПЕРСОНАЛЬНИХ ДАНИХ

У разі виявлення витоку персональних даних слід негайно вжити заходів для мінімізації ризиків та захисту постраждалих осіб. Детальна процедура реагування визначена в MV-PROC-ERP-001 (ІНЗ).

Ключові кроки:

Оцінка ситуації: визначити джерело та обсяг витоку; категорії залучених персональних даних; можливі наслідки для суб'єктів даних.

Негайні заходи: обмежити доступ до скомпрометованої системи; усунути причину витоку; за необхідності залучити фахівців з кібербезпеки.

Повідомлення органів:

- повідомити Кіберполіцію (якщо витік має ознаки кібератаки);
- повідомити Уповноваженого Верховної Ради з прав людини орган з захисту персональних даних – відповідно до вимог законодавства.
- за наявності ознак кіберінциденту в інформаційно-телекомунікаційній системі — додатково повідомити CERT-UA / Держспецзв'язку відповідно до Закону України «Про основні засади забезпечення кібербезпеки України».

Правові підстави повідомлення Уповноваженого: чинний Закон України «Про захист персональних даних» (№ 2297-VI) прямо не встановлює обов'язку повідомляти про сам факт витоку. Обов'язковим за ст. 9 Закону є лише повідомлення Уповноваженого про обробку категорій даних з особливим ризиком протягом 30 робочих днів з початку такої обробки та про зміну цих відомостей протягом 10 робочих днів. Повідомлення Уповноваженого про витік як такий Research.ua здійснює як добру практику для мінімізації ризиків відповідальності за ст. 24 Закону.

Застосування GDPR: якщо витік стосується персональних даних суб'єктів з країн ЄС (наприклад, респондентів чи клієнтів), додатково застосовуються обов'язкові строки GDPR: повідомлення надзорного органу протягом 72 годин (ст. 33 GDPR) та постраждалих осіб без невиправданої затримки у разі високого ризику (ст. 34 GDPR).

Моніторинг законодавчих змін: Компанія відстежує законопроєкт № 8153 «Про захист персональних даних» (гармонізований з GDPR, ухвалений у першому читанні 20.11.2024, готується до другого читання), який після набрання чинності запровадить прямий обов'язок повідомляти про витік і надзорний орган, і постраждалих суб'єктів у визначені строки. Ця Політика буде оновлена відповідно до нових вимог після ухвалення закону.

Інформування клієнтів та донорів: якщо витік стосується даних клієнта або донора – повідомити протягом 72 годин. Повідомлення здійснює CEO.

Інформування постраждалих осіб: повідомити суб'єктів персональних даних про ризики та надати рекомендації щодо захисних дій.

Розслідування та запобігання: провести внутрішнє розслідування; оновити процедури безпеки; провести навчання команди.

Відповідальні за реагування: COO (операційна координація), CTO (технічне усунення), CEO (зовнішня комунікація).

9. НАДАННЯ ІНФОРМАЦІЇ ТА ПЕРСОНАЛЬНИХ ДАНИХ ТРЕТІМ ОСОБАМ

Надання інформації та персональних даних третім особам регулюється законодавством України про захист персональних даних та міжнародними нормами, що гарантують конфіденційність і безпеку даних.

Загальні принципи передачі персональних даних:

- законність – передача відбувається на підставі законодавства або договору;
- прозорість – особа поінформована про передачу її даних;
- обмеження мети – передача можлива лише для цілей, визначених під час збору;
- мінімізація – передаються лише необхідні дані;
- безпека – дані захищені від несанкціонованого доступу при передачі.

Клієнти та донори Research.ua отримують виключно знеособлені масиви даних (без імен, телефонів, email респондентів), якщо інше не передбачено договором та явною згодою суб'єктів.

Передача персональних даних зовнішнім підрядникам (DP-менеджери, транскрибатори, кодувальники) здійснюється через захищені посилання Google Drive з обмеженим доступом. Передача через месенджери у незашифрованому вигляді заборонена.

Передача персональних даних заборонена:

- без явної згоди суб'єкта даних (крім випадків, передбачених законом);
- якщо це суперечить законодавству або умовам договору;
- якщо є ризик шкоди особі;
- з метою комерційного продажу або незаконного використання.

10. ВІДПОВІДАЛЬНІСТЬ

Відповідальність за реалізацію та дотримання цієї політики розподіляється між:

Роль	Відповідальність
CEO	Затвердження та перегляд цієї політики; рішення щодо зовнішньої комунікації при інцидентах ІБ.
COO	Власник та відповідальний за актуальність політики. Управління доступами в Google Workspace. Координація реагування на інциденти ІБ.
CTO	Технічна реалізація вимог безпеки. Управління резервними копіями. Технічне розслідування ІБ-інцидентів.
HR Manager	Ознайомлення нових співробітників та партнерів із цією політикою при onboarding; збір підписаних підтверджень.

Project Manager	Забезпечення дотримання вимог ІБ в межах своїх проєктів; ознайомлення залучених підрядників.
Усі співробітники та партнери	Особисте дотримання вимог цієї політики. Негайне повідомлення COO або CTO про будь-який підозрюваний інцидент ІБ.

Порушення цієї політики може мати наслідки:

- для штатних співробітників – дисциплінарні заходи аж до припинення трудових відносин;
- для ФОП-партнерів та підрядників – дострокове припинення договору та відшкодування збитків;
- для всіх – юридична відповідальність відповідно до законодавства України.

Ця політика надається на ознайомлення для всіх співробітників та залучених партнерів. Вимоги є обов'язковими до виконання.

Політика переглядається не рідше одного разу на рік або позапланово – при змінах у законодавстві, вимогах донорів або після суттєвого ІБ-інциденту.

Список затвердження:

Ім'я	Посада	Дата	Підпис
Ніна Делюкова	CEO (директор)	01.01.2026	
Олена Волкова	COO	01.01.2026	