ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Громадської організації «Центр досліджень і сприяння реформ» (ГО «ЦДСР»)

1. Мета та сфера застосування

Ця Політика встановлює єдині корпоративні стандарти Громадської організації «Центр досліджень і сприяння реформ» (надалі — ГО «ЦДСР») щодо збору, обробки, зберігання, використання та захисту інформації, зокрема персональних даних співробітників, експертів, волонтерів, партнерів, а також бенефіціарів та респондентів соціологічних і ринкових досліджень.

Метою документа є гарантування конфіденційності, цілісності та доступності інформаційних активів ГО «ЦДСР», захист прав суб'єктів персональних даних, а також забезпечення відповідності операційної та науково-дослідної діяльності суворим вимогам міжнародних донорів та стандартам прозорості OECD DAC.

2. Нормативно-правова база

Політика ґрунтується на вимогах:

- Закону України «Про захист персональних даних»;
- Закону України «Про інформацію»;
- Загального регламенту про захист даних Європейського Союзу (GDPR) — застосовується під час реалізації міжнародних грантових проєктів та партнерств із європейськими інституціями.

3. Категорії даних та принципи обробки

Організація обробляє такі категорії інформації:

- ***Кадрові та експертні дані*:** ПІБ, паспортні дані, РНОКПП, банківські реквізити, резюме (CV), контактні дані членів команди, підрядників та волонтерів.
- ***Дослідницькі дані (бенефіціари та респонденти)*:** Інформація,

зібрана під час польових досліджень, опитувань, фокус-груп та моніторингу реформ (може включати соціально-демографічні показники, статус ВПО тощо).

- ***Комерційна та грантова таємниця*:** Фінансова звітність, стратегічні плани, бази даних донорів, авторські методології та неопубліковані аналітичні звіти.

Обробка здійснюється на принципах законності, прозорості, мінімізації (збираються лише ті дані, які критично необхідні для конкретного проєкту) та обмеження терміну зберігання.

4. Отримання згоди та захист респондентів

Будь-який збір персональних даних здійснюється виключно за умови отримання добровільної, інформованої та однозначної згоди суб'єкта даних (у письмовій формі або через електронні форми підтвердження — чекбокси).

***Специфіка аналітичної роботи*:** Усі дані, зібрані в рамках соціологічних чи польових досліджень, підлягають обов'язковій *анонімізації* (знеособленню) перед їх використанням в аналітичних записках, публікаціях або звітах. ГО «ЦДСР» гарантує, що за опублікованими результатами неможливо ідентифікувати конкретну особу-респондента.

5. Зберігання даних та контроль доступу

- ***Цифрові активи*:** Бази даних, корпоративне листування та дослідницькі архіви зберігаються на захищених корпоративних хмарних серверах ГО «ЦДСР». Використання особистих незахищених дисків для зберігання чутливої проєктної інформації заборонено.
- ***Обмеження доступу*:** Доступ до персональних даних та фінансової інформації надається працівникам виключно за принципом «необхідно знати» (Role-Based Access Control) для виконання їхніх прямих посадових обов'язків.
- ***Кібергігієна*:** Усі облікові записи співробітників, що мають доступ до баз даних, повинні бути захищені складними паролями та двофакторною автентифікацією (2FA).

- ***Паперові архіви*:** Документи (договори, анкети, відомості) зберігаються у замкнених шафах або сейфах в офісі ГО «ЦДСР».

6. Передача даних третім особам та донорам

ГО «ЦДСР» не продає, не обмінює та не передає персональні дані стороннім особам у комерційних цілях. Передача баз даних з персональною інформацією бенефіціарів донорським організаціям або міжнародним партнерам здійснюється виключно за наявності попередньої письмової згоди самих бенефіціарів на таку передачу. Без згоди донорам надаються лише агреговані (статистичні) та знеособлені дані.

7. Права суб'єктів даних та знищення інформації

Кожна особа, чиї дані обробляє ГО «ЦДСР», має право на доступ до своїх даних, виправлення неточностей, а також право вимагати їх видалення («право бути забутим»). Запити на видалення розглядаються керівництвом ГО протягом 5 робочих днів.

Після завершення строку зберігання, визначеного законодавством або правилами грантової угоди (наприклад, після завершення періоду пост-проєктного аудиту), документи, що містять персональні дані, підлягають безпечному знищенню (паперові — через шредер, цифрові — шляхом безповоротного видалення з серверів).

8. Дії у випадку витоку даних

У разі виявлення факту несанкціонованого доступу, кібератаки, втрати пристроїв з корпоративною інформацією або витоку баз даних, працівник зобов'язаний негайно сповістити Виконавчого директора. Керівництво ГО «ЦДСР» протягом 72 годин проводить внутрішнє розслідування, блокує скомпрометовані доступи та, у разі загрози правам осіб, повідомляє про інцидент суб'єктів даних та відповідних стейкхолдерів (донорів).

9. Відповідальність

Персональну відповідальність за організацію системи захисту інформації

несе Виконавчий директор ГО «ЦДСР». Кожен працівник, експерт або волонтер несе особисту дисциплінарну, цивільну чи кримінальну відповідальність за умисне розголошення персональних даних, комерційної таємниці або порушення правил інформаційної гігієни.

З Політикою інформаційної безпеки та захисту персональних даних ознайомлений(а) та зобов’язуюсь її суворо дотримуватись:

ПІБ:

_____

Посада / Роль в ГО «ЦДСР»:

_____

Дата: «____» _____ 20___ р. Підпис: _____