The Tenth of April
Громадська організація «Десяте квітня»

Захист персональних даних: важливі кроки та рішення

Дорожня карта для громадських організацій, які опікуються питаннями розвитку громад та спільнот ВПО

Цю публікацію було підготовлено за підтримки Агентства ООН у справах біженців (UNHCR). Зміст цієї публікації є виключно відповідальністю ГО «ДЕСЯТЕ КВІТНЯ» і не може використовуватися для відображення точки зору Агентства.

Авторка: Уляна Шадська
Юристка, консультантка міжнародних організацій та технологічних компаній з питань цифрового законодавства. Авторка видань у сфері захисту персональних даних.

ЗМІСТ

ВСТУП

У січні 2011 року набрав чинності Закон «Про захист персональних даних», який зобов'язує тих, хто збирає дані, забезпечити їх належний захист. Хоч вже пройшло багато часу, але дотепер точаться дискусії, які кроки необхідно зробити, аби створити в Україні належну систему захисту персональних даних.

Особливо гостро постало це питання під час пандемії COVID-19, коли великими темпами почала розвиватися діджиталізація усіх сфер життєдіяльності. Державні органи, бізнес та громадські організації намагаються здійснювати свою роботу дистанційно за допомогою мережі інтернет. Цифрова трансформація передбачає збір та використання персональних даних, що викликає занепокоєння у суспільства, адже несанкціонований виток особистої інформації може нести ризики для людини.

Це означає, що розвиток технологій поступово змінює не тільки спосіб комунікації, а й формує нові індикатори оцінки діяльності організацій. Усі масштабні опитування, які проводять у різних куточках світу, доводять той факт, що захист персональних даних — стає новим критерієм довіри.

Громадські організації — є рушієм реформ та суспільних змін, тому на власному прикладі мають показувати, як формується демократичне суспільство, де є повага до приватності людини. Для цього потрібно докласти максимум зусиль, щоби зрозуміти практичні аспекти впровадження національного та міжнародного законодавства.

Немає єдиного шаблону як організувати процес обробки та захисту персональних даних, бо кожна організація унікальна за своєю специфікою діяльності. Тому потрібно самостійно працювати над тим, щоби безпека конфіденційної інформації стала частиною внутрішньої культури. Це стане важливим кроком не тільки для конкретної спільноти, а й держави у цілому, на шляху до реформи у даній сфері.

Цей документ — «дорожня карта» для громадських організації, що опікуються питаннями розвитку громад та спільнотами ВПО, у якому описані загальні положення законодавства та послідовний спектр дій, що варто зробити, аби забезпечити захист персональних даних. Очікується, що в результаті роботи з даним методичним матеріалом, організації посилять свою спроможність дотримуватися вимог закону та зможуть продемонструвати суспільству, що вони поважають право приватне життя кожної людини.

[1] **Внутрішньо переміщені особи (ВПО)** — люди, які залишили свої домівки, рятуючись від небезпеки, але не перетнули міжнародний кордон, а залишились на території рідної країни.

ТЕРМІНИ

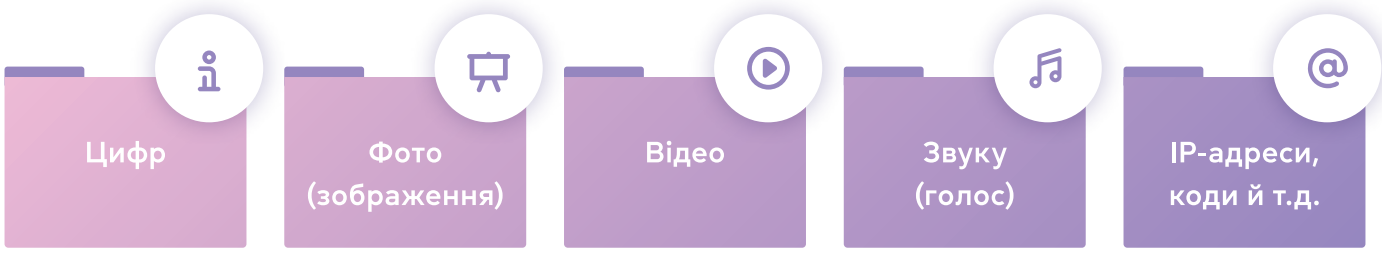
1.1. Що таке «персональні дані»?

Персональні дані – це відомості чи сукупність відомостей про фізичну особу, які дають можливість прямо або опосередковано її ідентифікувати.

Від правильного розуміння цього та інших пов'язаних з ним понять, залежить те, наскільки законною буде діяльність організації у даній сфері. На перший погляд, формулювання може здаватися простим, але на практиці часто потребує роз'яснення. Для кращого сприйняття розділимо його на змістовні блоки:

- **«будь-які відомості, що стосуються фізичної особи»**

Є помилкове уявлення, що йдеться тільки про паспорт, ідентифікаційний код або номер телефону. Насправді, це стосується будь-якої інформації про людину, яка відображає її фізичну, генетичну, соціальну або культурну ідентичність. Персональні дані можуть бути виражені у формі:



- **«яка ідентифікована або може бути конкретно ідентифікована»**

Особа вважається «ідентифікованою» або «яка може бути ідентифікована», якщо її або його можна відрізнити від інших людей. Скажімо, коли на паркані є надпис з ім'ям й не зрозуміло про кого йде мова, у такому випадку це не буде вважатися персональними даними. Лише тоді, коли ця інформація поєднуватиметься з іншою, яка надасть змогу визначити конкретну особу. Законодавець розділив загальний масив інформації про людину на загальну та ту, що може нести особливий ризик для прав і свобод людини.

До **загальної категорії** відносять інформацію про прізвище та ім'я, дату та місце народження людини, її зображення, сімейний стан, майно, адресу місця проживання, професію тощо.

Особлива категорія розкриває інформацію про расове або етнічне походження, політичні та релігійні переконання, приналежність до політичних партій, наявність судимості за вчинення правопорушення, а також дані, що стосуються здоров'я, статевого життя, біометричних особливостей[3].

[2] Стаття 2 Закону «Про захист персональних даних»

[3] У статті 7 Закону про захист даних «Особливі вимоги до обробки персональних даних» вказується вичерпний перелік особливої категорії даних.

Наприклад, внутрішньо переміщені особи (ВПО) — люди, що залишили свої домівки, рятуючись від небезпеки, але не перетнули міжнародний кордон, а знаходяться на території рідної країни. Сам по собі статус ВПО може не належати до особливої категорії даних, але у поєднанні з іншою інформацію, скажімо світоглядні та політичні переконання людини вже є підставою, щоби вважати таку інформацію, яка може нести для неї особливий ризик (тобто, особлива категорія даних).

У разі якщо формується база, де містяться інформація особливої категорії даних, потрібно повідомити про це Уповноваженого Верховної Ради України з прав людини. З порядком повідомлення можна ознайомитися на офіційному сайті Омбудсмана.

1.2. Що таке обробка персональних даних?[5]

Обробка персональних даних — це не лише збирання або накопичення інформації. Мова йде про будь-яку дію: збирання, реєстрація, зберігання, накопичування, адаптування, зміна, поновлення, використання, поширення, реалізація, передача, знеособлення, знищення.

[5] Стаття 2 Закону «Про захист персональних даних».

1.3. Учасники відносин пов'язаних з персональними даними[6]

1. Суб'єкт персональних даних – фізична особа, чиї персональні дані обробляються.
2. Володілець персональних даних – фізична або юридична особа, яка збирає дані, визначає мету, встановлює спосіб та порядок їх обробки, та має у власності відповідне технічне обладнання. Володільцями персональних даних можуть бути підприємства, установи і організації усіх форм власності, органи державної влади чи органи місцевого самоврядування, а також фізичні особи-підприємці.
Наприклад, якщо спільнота організацій (коаліція ВПО) або ініціативна група незареєстрована як окрема юридична особа, але в рамках своєї діяльності збирає персональні дані, тоді такий суб'єкт також може вважатися — володільцем даних. Питання полягає у законних підставах та меті такої діяльності (про це детальніше у наступних розділах).
3. Розпорядник персональних даних – фізична чи юридична особа, якій договором або законом надано право володільцем даних їх обробляти.
Наприклад, громадська організація збирає персональні дані (володілець даних) та передає їх за договором організації-підряднику (розпорядник даних) для виконання певних функцій (організації заходів, закупівлі обладнання, оформлення робочої подорожі тощо).
Але важливо те, що розпорядник повинен обробляти дані лише з метою і в обсязі, які були визначені договором.
Індикатори, за якими можна визначити, коли організація є володільцем чи розпорядником персональних даних (за договором):

Володілець

1. Першочергово збирає та обробляє персональні дані.
2. Визначає мету або результат обробки даних.
3. Вирішує, яку категорію даних потрібно збирати (відповідно до мети).
4. Обробляє дані в результаті договору (або за згодою) безпосередньо між суб'єктом даних.
5. Самостійно приймає рішення щодо того, кому будуть передані дані (за умови згоди суб'єкта даних, якщо інше не визначено законом).
6. Має право укладати угоди щодо передачі даних від свого імені.

Розпорядник

1. Отримує від володільця.
2. Обробляє інформацію виключно з тією метою та у тому об'ємі, що була визначена володільцем.
3. Працює лише з тими даними, які було передано володільцем (або визначено законом).
4. Обробляє персональні дані за договором (або законом) між володільцем даних.
5. Обробляє дані виключно в рамках умов договору між володільцем даних.
6. Тільки, якщо це передбачено умовами договору між володільцем даних.

[6] Стаття 4 Закону «Про захист персональних даних»

ПРИНЦИ

4. Уповноважений Верховної Ради України з прав людини (Омбудсман) — здійснює контроль за дотриманням законодавства у даній сфері.

5. Третя особа — будь-яка особа (за винятком суб'єкта даних та Омбудсмана), якій володілець чи розпорядник передає персональні дані.

Наприклад, до громадської організації звернувся державний орган, установа чи організація (або будь-хто інший) про отримання інформації (персональних даних), що збираються. У такому випадку цей орган буде вважатися третьою особою.

1.4. Принципи обробки персональних даних

Міжнародні стандарти визначають принципи обробки персональних даних, які за своєю сутністю є фундаментом для врегулювання цієї сфери. Будь-який процес роботи з інформацією буде опиратися на ці правила.

1. Законність, справедливість та прозорість.

Законність обробки персональних даних передбачає те, що дані обробляються лише у законний спосіб, для законних цілей і за наявності правових засад для цього. Будь-яка робота з даними за відсутності легітимних підстав, забороняється.

Справедливість полягає у обов'язковому врахуванні прав суб'єкта персональних даних при їх обробці, унеможливленні завдання шкоди його законним інтересам.

Прозорість гарантує кожному отримання повної та достовірної інформації про обробку своїх персональних даних та безпосередній доступ до них. Тобто, організації повинні пояснювати у доступній формі: для чого і яким чином отримує дані, як планує використовувати та кому вони можуть бути передані.

2. Обмеження мети.

Персональні дані можуть збиратися лише з конкретною та законною метою й за умов, коли без цих даних досягнення такої мети неможливе. Саме мета має визначати обсяг та спосіб обробки даних, а не навпаки. Принцип обмеження мети вимагає заздалегідь визначити, обґрунтувати реальні підстави й мету збору даних, адже надалі це стане запобіжником від їх використання у незаконних цілях.

Наприклад, якщо організація влаштовує захід і їй необхідні номери телефонів учасників для його проведення, тоді ці дані не можуть використовуватися для інших цілей. Скажімо, для реклами своїх послуг або передаватися партнерам для розширення бази контактів.

3. Мінімізація даних.

Принцип мінімізації, який тісно пов'язаний з принципом обмеження мети, полягає у тому, що обсяг отримуваних даних має бути зменшений до мінімального рівня. Володілець може збирати лише ті дані, які забезпечують досягнення цілей їх обробки, і не більше.

Наприклад, якщо організація збирає контакті дані (електронні адреси та номери телефонів) виключно для комунікації зі своєю цільовою аудиторією, то їй не потрібно отримувати додаткову інформацію, скажімо про релігійні вподобання.

4.Точність.

Цей принцип вимагає від організації постійного контролю за точністю, достовірністю та актуальністю отриманих персональних даних. Застарілі або неточні дані підлягають невідкладному виправленню або знищенню у такий спосіб, що виключає можливість їх поновлення.

5. Обмеження строку зберігання.

Персональні дані мають зберігатися не довше, ніж це необхідно для досягнення мети їх обробки — як тільки таку мету досягнуто, дані повинні бути видалені. Зберігання інформації протягом більш тривалого часу допускається виключно з метою реалізації громадських інтересів, у наукових цілях, задля історичних досліджень або формування статистики. Також, у разі необхідності, тривале зберігання даних можна здійснювати після їх знеособлення — тобто приведення у вигляд, який унеможливлює ідентифікацію особи.

6. Цілісність і конфіденційність (безпека).

Обробка даних повинна здійснюватися у спосіб, який гарантує їх належну безпеку, в тому числі захист від несанкціонованої/незаконної або випадкової втрати. Організація несе повну відповідальність за реалізацію таких заходів, які мають бути співмірними до ризиків всіх можливих порушень у даній сфері.

7. Підзвітність.

Організація, яка обробляє персональні дані, повинна демонструвати правомірність здійснення своєї діяльності. Підзвітність — це не лише пред'явлення звітів про роботу контролюючим структурам. У широкому розумінні — це ознайомлення суспільства з тим, яким чином забезпечується захист зібраної інформації у діяльності конкретної організації. Дотримання цього принципу допомагає отримати довіру людей, оскільки наочно демонструє, що організація поважає приватне життя людини, виконує вимоги законодавства та готова нести відповідальність за свої дії. Тому, необхідно прийняти відповідні технічні та організаційні заходи для виконання вимог підзвітності.

Наприклад, серед таких заходів може бути прийняття та публікація на сайті політики обробки та захисту даних; періодичне інформування суспільства про свою діяльність з обробки та захисту даних, зокрема про умови договорів з організаціями, які обробляють дані від імені організації; інформування про інциденти, які виникли у наслідок витоку персональних даних; призначення відповідальних осіб за обробку даних тощо.

Підсумовуючи, можна зауважити, що вказані принципи пов'язані й доповнюють один одного, утворюючи єдину концепцію дотримання прав і свобод людини при обробці персональних даних.

1.5. Підстави для обробки персональних даних

Дуже важливо відповісти на це питання та застосовувати правильну підставу, адже саме від цього буде залежати чи законно збирається інформація. Закон визначає перелік підстав, коли можна збирати персональні дані:

1. Згода суб'єкта персональних даних на обробку інформації про себе;
2. Дозвіл на обробку персональних даних, наданий володільцю персональних даних відповідно до закону виключно для здійснення його повноважень;
3. Укладення та виконання правочину, стороною якого є суб'єкт персональних даних або який укладено на його користь;
4. Захист життєво важливих інтересів суб'єкта персональних даних;
5. Необхідність виконання обов'язку володільця даних, який передбачений законом;
6. Необхідність захисту законних інтересів володільця персональних даних або третьої особи, якій передаються дані, крім випадків, коли потреби захисту основоположних прав суб'єкта персональних даних у зв'язку з обробкою його даних переважають такі інтереси[7].

Наприклад, у контексті роботи громадських організацій з цього переліку найбільш прийнятною підставою для обробки даних можна вважати буде — згода суб'єкта, чиї дані збираються.

[7] Стаття 11 Закону «Про захист персональних даних»

1.6. Що означає згода суб'єкта персональних даних?

Це надання дозволу з боку фізичної особи на обробку своїх персональних даних[8]. Можна виділити декілька способів отримання згоди від особи:

1. Згода надана у письмовому/електронному вигляді.

Наприклад, коли для проведення публічного заходу організація збирає контактні дані учасників через онлайн форму, тоді там має бути повідомлення про подальшу обробку даних із запитом чи погоджується особа, яка передає про себе інформацію.

2. Усна згода. Особа може в усній формі виразити свою згоду.

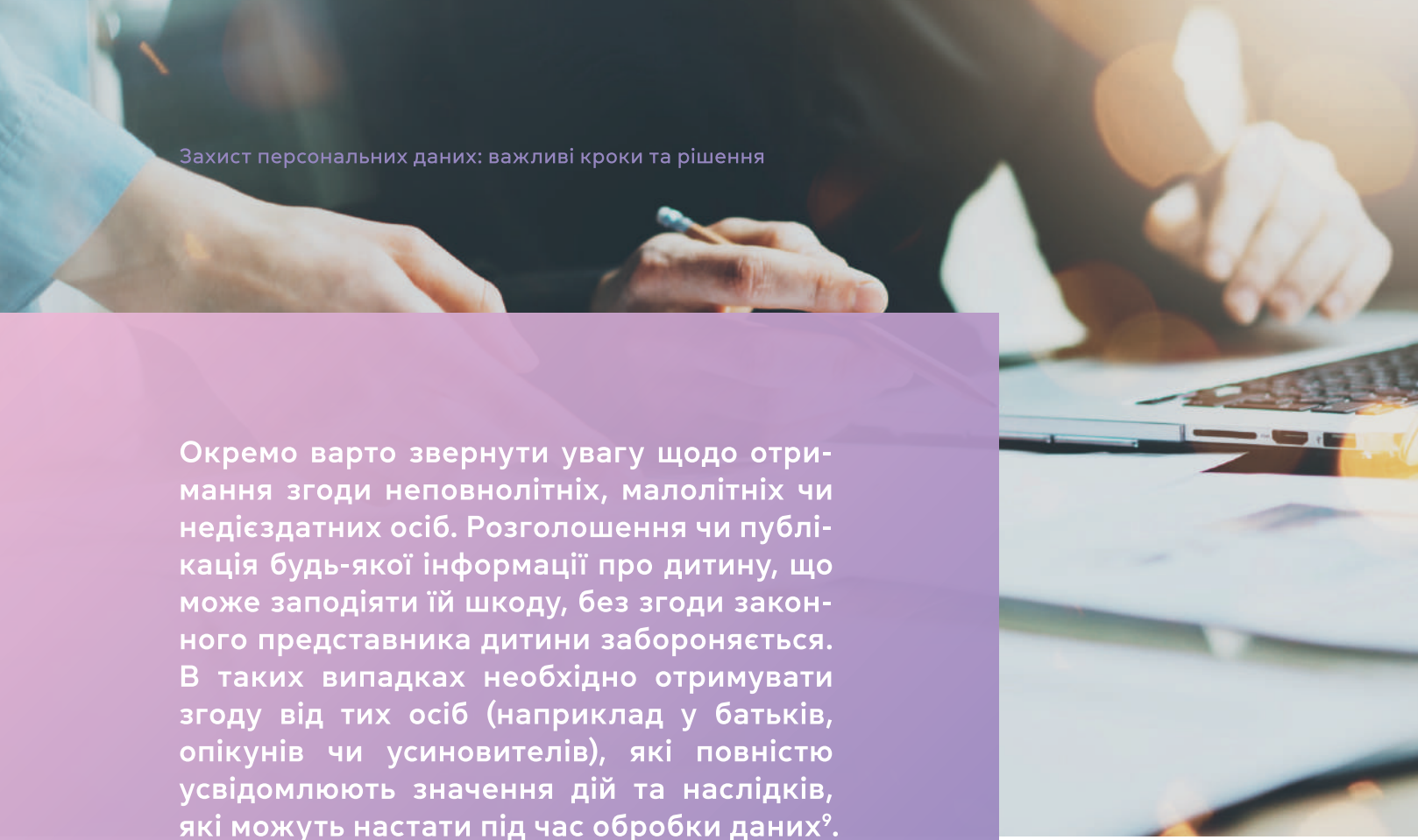
Наприклад, якщо під час онлайн наради від організації вирішили зробити скріншот екрану комп'ютера (чи телефону) із зображенням присутніх на зустрічі, тоді обов'язково потрібно запитати осіб чи вони не проти цього, зокрема щодо подальшого використання зображення (публікації в мережі тощо).

3. Мовчазна згода. Коли особа була попереджена, але не виразила своїх заперечень.

Часто виникають питання саме щодо застосування принципу «мовчазної згоди». Давайте змоделюємо ситуацію. На заході, наприклад, тренінгу, фотограф від організації зайшов у зал, аби зробити фото. У залі люди побачили його і не заперечили проти цього, тобто надали мовчазну згоду. Але в будь-якому випадку, особа має право звернутися з вимогою про видалення світлин чи відео з її участю. Застосування цього принципу потребує максимальної відкритості процесу — фотокамери не повинні приховуватися (роботи це так, щоб особа не помітила фотозйомку).

Разом з тим, не заперечення проти зйомки, ще не означає надання згоди на публікацію світлин або відео в мережі. Про це потрібно питати окремо.

[8] Стаття 2 Закону «Про захист персональних даних»



Окремо варто звернути увагу щодо отримання згоди неповнолітніх, малолітніх чи недієздатних осіб. Розголошення чи публікація будь-якої інформації про дитину, що може заподіяти їй шкоду, без згоди законного представника дитини забороняється. В таких випадках необхідно отримувати згоду від тих осіб (наприклад у батьків, опікунів чи усиновителів), які повністю усвідомлюють значення дій та наслідків, які можуть настати під час обробки даних[9].

А також, для того, щоб відповідати Закону, згода повинна мати такі ознаки:

- **Поінформованість** передбачає, що особі надано інформацію про те, ким та з якою метою будуть оброблятися її персональні дані, а також умови їх захисту.
- **Добровільність.** Особи, чиї дані збираються, мають право самостійно вирішувати, чи давати на це згоду або ні. Суб'єкт може відкликати згоду на обробку персональних даних, окрім випадків передбачених законом[10].

1.7. Відповідальність за порушення вимог законодавства

Контроль за додержанням законодавства у цій сфері здійснюють Уповноважений Верховної Ради України з прав людини та суди[11]. Порушення законодавства про захист даних тягне за собою відповідальність, встановлену законом[12].

[9] Стаття 10 Закону «Про охорону дитинства»

[10] Стаття 8 Закону «Про захист персональних даних».

[11] Стаття 22 Закону «Про захист персональних даних»

Зокрема:
1. Кодексом України про адміністративні правопорушення (статтею 188-39 «Порушення законодавства у сфері захисту персональних даних»). КУпАП передбачає покарання у вигляді адміністративного штрафу як за ігнорування вимог Уповноваженого, так і за недодержання порядку захисту персональних даних.
2. Кримінальним кодексом України (статтями 182 «Порушення недоторканності приватного життя» та 359 «Незаконні придбання, збут або використання спеціальних технічних засобів отримання інформації»).

КРОКИ

Робота із захистом персональних даних: головні кроки

Забезпечення захисту персональних даних — це вимога, визначена законом. Якщо організація ігнорує ці зобов'язання, тоді її діяльність не можна назвати законною та претендувати на суспільну довіру та повагу. Початок роботи з обробки та захисту даних умовно можна розділити на три етапи:

- По-перше, зробити базові кроки для організації процесу обробки даних.
- По-друге, подбати про права осіб, чиї дані збираються.
- По-третє, подумати про безпеку цієї інформації.

II. Організація процесу управління даними

01 крок **Зробити аналіз діяльності.**

02 крок **Визначити мету та законні підстави збору даних**

03 крок **Розробити документи**

04 крок **Подбати про права осіб**

05 крок **Сформувати правила доступу до даних третіх осіб**

06 крок **Упорядкувати договірні відносини з розпорядниками**

07 крок **Призначити відповідальних осіб**

08 крок **Встановити правила накопичення та строк зберігання даниха осіб**

2.1. Зробити аудит та скласти список персональних даних

Аудит діяльності організації у даній сфері має дати відповідь на питання: **«Що у вас робиться з персональними даними?»**. Розібратися, хто, що і з якою метою збирали, що потрібно залишити, або що знищити. У контексті роботи громадських організацій ВПО, такий аналіз може виглядати через складання форми:

№	Питання для аналізу діяльності	Відповідь	Примітка (приклад)
1	На якій підставі здійснює свою діяльність організація?	+	Статут, Положення, закон тощо.
2	Які категорії та вид персональних даних збирається/обробляються?	+	Загальна категорія: ПІБ, номери телефонів, електронні адреси тощо. Особлива: політичні переконання, світогляд.
3	Категорії осіб, чиї дані збираються?	+	Працівники/ці або члени/кині організації, ВПО, громадські активісти/ки та ін.
4	З якою метою збираються дані?	+	Потрібно вказати конкретну мету під кожну категорію даних, у разі, якщо вона відрізняється.
5	З яких джерел збирається інформація?		Скажімо, веб-сайт, гугл-форма, під час заходів тощо.
6	На якій законній підставі збирається інформація?		Згода особи, чиї дані збираються чи інше.
7	Яка форма отримання згоди?		Відмітка в електронному файлі, паперовому носії чи інше.
8	Яким чином забезпечується доступ осіб до своїх персональних даних?		Вказати можливі способи надання інформації (особисто, поштою, через веб-сайт)
9	Яка форма обробки персональних даних?		Паперова, за допомогою інформаційних систем (комп'ютерних програм) тощо.
10	Хто бере участь в обробці даних та хто до них має доступ?		Кількість осіб, та хто конкретно з працівників/членів громадської організації працює з даними.
11	Хто відповідальна особа?		Назва посади та процедура призначення (згідно статуту, посадової інструкції чи спільного рішення членів/кинь організації)
12	Де зберігається інформація?		Усі можливі носії: комп'ютери, флеш-пам'ять, накопичувач, електронна пошта, гугл-диск тощо.

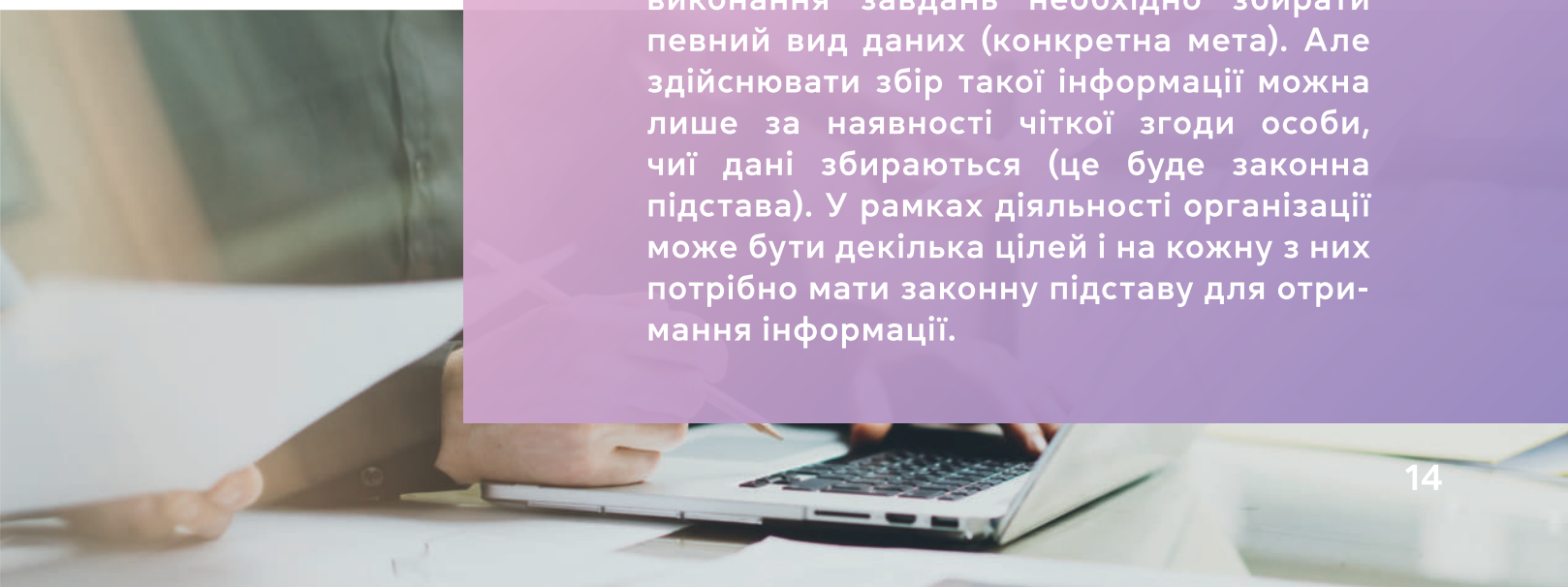
13	Хто власник бази даних?	Громадська організація чи інформація міститься на приватних комп'ютерах (інших носіях).
14	Чи здійснювалась передача даних на вимогу третіх осіб?	Вказати інформацію: коли та на якій підставі були передані дані. Наприклад, звернення правоохоронних органів, адвокатський запит тощо.
15	Який термін зберігання та чи він десь визначений?	Потрібно зазначити конкретний, аргументований строк.
16	Які можуть бути ризики витоку даних?	Перелік можливих сценаріїв витоку даних.
17	У якій спосіб знищується інформація?	Видаляються з комп'ютерів тощо.

Потрібно відверто відповісти на ці запитання, адже таким чином можна зрозуміти у чому проблема та визначити загальну стратегію роботи з даними.

2.2. Визначити мету та законні підстави обробки даних

Як вже було зазначено раніше, організації, що збирають персональні дані, повинні бути в змозі відповісти на питання, з якою метою вони це роблять та на яких законних підставах. Отже, просто так збирати інформацію не можна, потрібно обґрунтувати такі дії. Саме від цього буде залежати обсяг та спосіб обробки даних, а не навпаки.

Наприклад, громадська організація діє на підставі статуту, відповідно до якого для виконання завдань необхідно збирати певний вид даних (конкретна мета). Але здійснювати збір такої інформації можна лише за наявності чіткої згоди особи, чиї дані збираються (це буде законна підстава). У рамках діяльності організації може бути декілька цілей і на кожну з них потрібно мати законну підставу для отримання інформації.



2.3. Задокументувати усі процеси обробки даних

Обробка персональних даних — це процес, який складається з певних етапів, що має регулюватися відповідними внутрішніми документами. Тобто після того, як буде проведено аналіз, які дані організація збирає та для чого, усі ці процеси потрібно задокументувати. Особливо важливо налагодити процедури щодо передачі даних до третіх осіб. Тобто, якщо організація ділиться з кимось даними, необхідно узгодити правову основу та проаналізувати спроможність особи, якій передає дані, належно забезпечити їх безпеку.

Немає вичерпного переліку необхідного пакету документів. Все залежить від специфіки діяльності та повноважень організації, набору функцій інформаційних систем (якщо здійснюється автоматизована обробка даних), кількості персоналу, залученого до роботи з даними тощо. Як правило, керівництво організації самостійно вирішує, які необхідні положення та як здійснювати менеджмент управління даними.

Але, серед головних документів, який буде демонструвати процедури обробки даних в організації, тим самим підтверджуючи її прозорість та підзвітність — «Політика обробки персональних даних» (або ще «Політики приватності»). У такому документі мають бути зрозумілою мовою детально розписані усі організаційні та технічні заходи обробки персональних даних.

Наприклад, спробуємо скласти приблизну структуру такого документа. Що він має містити?

1. Загальні положення:

- мета обробки даних;
- види та категорії даних, що збираються;
- законна підстава;
- область застосування;
- терміни та визначення (які застосовуються у документі);

01

2. Права суб'єкта даних:

- інформування (про що та у якій формі організація інформує осіб, чиї дані збирає);
- право на доступ до своїх даних;
- право на виправлення та видалення даних;
- право на заперечення;
- процедура розгляду запитів;
- виключення (які є винятки, коли організація не може виконати вимоги суб'єкта даних).

02

3. Процедури обробки персональних даних:

- інформаційні системи (а також програми), задіяні у процесі обробки даних;
- оцінка ризиків;
- заходи безпеки, які здійснює організація;
- несанкціонованого витоку інформації;
- забезпечення точності даних;
- термін зберігання інформації;
- порядок знищення інформації.

03

4. Обробка даних, що здійснюється партнерами (розпорядниками даних):

- загальні положення про умови передачі даних;
- перевірка щодо виконання вимог щодо захисту даних;
- припинення партнерства;

04

5. Передача персональних даних третім особам:

- загальні положення щодо процедур передачі даних;
- угоди про передачу даних;
- передача даних на вимогу третіх осіб (наприклад, правоохоронним органам);
- здійснення підзвітності та контролю.

05

6. Внутрішній контроль:

- особа, відповідальна за безпеку даних;
- проведення перевірок щодо дотримання правил безпеки при обробці персональних даних.

06

Важливо! Часто на практиці політику приватності (privacy policy) помилково перекладають як «політика конфіденційності». Але у чому тут помилка?

По-перше, конфіденційність — це один з елементів приватності, згідно з яким інформація захищена від витоку даних. Тобто, в політиці конфіденційності організація пояснює яким чином захистила доступ до конкретних даних, наприклад, коли людина відвідала сайт. Політика приватності ж — це про контроль всього процесу обробки даних від збору до знищення. Також можна використовувати назву «політика захисту персональних даних». Головне — назва повинна відображати зміст документа, у якому визначені завдання збору інформації, її вид, правові підстави й процедури обробки даних, права людей і обов'язки. З метою забезпечення принципів «прозорості» і «підзвітності», Політика обробки персональних даних та інші документи у цій сфері бажано, щоби були оприлюднені на офіційному сайті організації або доступні для ознайомлення у інший спосіб.

2.4. Розробити правила доступу до персональних даних третіх осіб

Персональні дані можуть стати предметом інтересу третіх осіб, які не беруть безпосередньої участі у їх обробці. Наприклад, правоохоронних органів, різних служб та відомств. Тому організація, яка є володільцем персональних даних, повинна встановити чіткі правила, коли, як та на якій підставі може їх передавати. Це важливо, адже умови та процедура надання третім особам доступу до інформації здійснюється не на власний розсуд, а лише у визначений законом спосіб та при наявності відповідних правових підстав.

Слід пам'ятати, **що обов'язок забезпечити належний захист інформації покладається на сторону, яка її поширює чи передає**. Тобто, коли організація передає персональні дані, то несе відповідальність за те, яким чином їх буде використано надалі та чи не призведе це до порушення законодавства.

У Законі наголошено про те, що доступ до персональних даних третій особі не надається, якщо вона відмовляється взяти на себе зобов'язання щодо забезпечення належного їх захисту. Окрім того, передавати інформацію можна за умови згоди суб'єкта персональних даних на їх обробку[13].

Наприклад, організація отримала запит з проханнями надати номери телефонів жінок ВПО з метою проведення соціологічного дослідження. Як має діяти організація?

По-перше, такий запит має містити таку інформацію:

1. якщо заявник фізична особа: прізвище, ім'я та по батькові, місце проживання (місце перебування) і реквізити документа, що посвідчує особу, яка подає запит);
2. якщо заявник юридична особа: найменування, місцезнаходження особи, яка подає запит, посада, прізвище, ім'я та по батькові особи, яка засвідчує запит; підтвердження того, що зміст запиту відповідає повноваженням особи;
3. прізвище, ім'я та по батькові, а також інші відомості, що дають змогу ідентифікувати фізичну особу, стосовно якої робиться запит;
4. відомості про базу персональних даних, стосовно якої подається запит, чи відомості про володільця чи розпорядника даних;
5. перелік персональних даних, що запитуються;
6. мета та/або правові підстави для запиту.

По-друге, для передачі такої інформації потрібно отримати згоду осіб, чиї персональні дані запитуються.

Звичайно, є виключення, якщо персональні дані запитуються за запитом:

1. для виконання завдань оперативно-розшукової чи контррозвідувальної діяльності, боротьби з тероризмом;
2. під час виконання органами державної влади та органами місцевого самоврядування своїх повноважень, передбачених законом;
3. якщо персональні дані обробляються в історичних, статистичних чи наукових цілях;
4. коли суб'єкт персональних даних ще під час їх збору був повідомлений про третіх осіб, яким можуть бути передані його дані.

[13] Стаття 16 Закону «Про захист персональних даних».

Порядок передачі персональних даних правоохоронним органам роз'яснений Офісом Омбудсмана[14], де вказується, що належною підставою для отримання правоохоронними органами доступу до персональних даних в рамках кримінального провадження є **ухвала слідчого судді**, суду про тимчасовий доступ до речей і документів. Усі інші запити на доступ до даних мають розглядатися індивідуально з огляду на повноваження запитувача, підстави запиту, обсяг запитуваної інформації тощо.

Окрім того, важливо зазначити, що у статті 19 Конституції встановлено, що органи державної влади та органи місцевого самоврядування, їх посадові особи зобов'язані діяти лише на підставі, в межах повноважень та у спосіб, що передбачені Конституцією та законами України. З огляду на це положення, третя особа (державний орган) може отримати персональні дані (або будь-які дії із ними) лише за наявності:

- повноважень;
- законної підстави;
- обґрунтованої мети;
- у спосіб, передбачений законом.

Тобто, не достатньо мати повноваження, має бути обґрунтована мета, підстава та чітка процедура.

Який строк розгляду такого запиту?

Строк вивчення запиту не може перевищувати 10 робочих днів з дня його надходження. Протягом цього строку треба повідомити особу, яка подала запит, чи буде його задоволено або чому запитувані персональні дані не підлягають наданню (із зазначенням підстави). Запит задовольняється протягом 30 календарних днів з дня його надходження, якщо інше не передбачено законом. Якщо потрібно більше часу для розгляду запиту, то закон дозволяє відстрочення строку до 45 днів, але при цьому, про це потрібно повідомити запитувача[15].

У повідомленні про відстрочення зазначаються:

- прізвище, ім'я та по батькові особи, яка приймає рішення про відстрочення;
- дата відправлення повідомлення;
- причина відстрочення;
- строк, протягом якого буде задоволено запит.

Чи може бути відмовлено у наданні даних?

Так, може бути відмовлено, якщо доступ до даних заборонено згідно із законом. Відмова оформлюється відповідним повідомленням, у якому зазначаються:

- прізвище, ім'я, по батькові особи, яка відмовляє у доступі;
- дата відправлення повідомлення;
- причина відмови.

Важливо! Відстрочення доступу суб'єкта персональних даних до своїх даних не допускається.

[14] **Щодо правових підстав передачі персональних даних правоохоронним органам:** http://www.ombudsman.gov.ua/ua/publication/petition/schodo-pravovix-pidstav-peredachi-personalnix-danix-pravooxoronnim-organam/

[15] **Стаття 17 Закону «Про захист персональних даних»**

2.5. Упорядкувати договірні відносини з розпорядниками

Якщо організації необхідно передати персональні дані розпоряднику, тоді треба розробити документ (договір), у якому будуть описані процедури обробки та захисту інформації. Контракт важливий для того, щоб обидві сторони розуміли свої зобов'язання.
Наприклад, організація планує провести публічний захід та передає логістичній компанії контактні дані учасників. Варто звернути увагу, що на це має бути попередня згода суб'єкта персональних даних. Інколи це не просто номери телефонів чи електронні адреси, а ще інформація про харчові звички, потреби або здоров'я людини.
Тому, розпорядники інформації повинні дотримуватися законодавства про захист даних.

Наприклад, що має включати такий договір (або іншому правовому акті)?

1. Деталі обробки даних, включаючи:
- предмет обробки даних;
- тривалість обробки;
- характер і мета обробки;
- тип персональних даних;
- категорії суб'єктів даних;
- обов'язки і права організації-володільця даних.

2. Умови або положення про зобов'язання розпорядника, який повинен:
- діяти відповідно до задокументованих інструкцій організації-володільця даних, за винятком випадків, коли закон вимагає діяти без таких інструкцій;
- гарантувати безпеку даних під час їх обробки;
- вживати відповідних заходів для забезпечення безпеки обробки;
- залучати сторонніх осіб тільки з попереднього дозволу організації-володільця даних і відповідно до договору;
- вжити відповідних заходів, щоб у разі потреби допомогти організації-володільцю даних відповісти на запити окремих осіб про здійснення своїх прав;
- видалити (або повернути) усі персональні дані після завершення дії договору, якщо закон не вимагає їх зберігання;
- проходити аудити та інспекції (у разі потреби).

2.6. Підвищити кваліфікацію

Складно недооцінити важливість підвищення кваліфікації у сфері захисту даних. У зв'язку зі швидким розвитком технологій, ця галузь права є дуже динамічною. Тому в організації повинні систематично проводитися навчання з питань захисту даних та інформаційної безпеки. Також слід навчитися розпізнавати поширені загрози, такі як фішингові повідомлення електронної пошти й зараження шкідливим програмами (вірусами). **(У Додатку №1 перелік корисних посилань у даній сфері).**

2.7. Призначити відповідальну особу за захист персональних даних

Закон покладає обов'язок створити підрозділ або призначити відповідальну особу, яка буде організовувати роботу, пов'язану із захистом персональних даних[16]. Часто у громадських організацій немає потреби створювати окремі відділи, але, в кожному випадку, варто визначити особу, яка буде відповідати за обробку та захист інформації. Немає конкретних вимог до посади, рівня освіти, кваліфікації особи, лише визначено, що вона або він повинні:

- інформувати з питань додержання законодавства про захист персональних даних;
- взаємодіяти з Омбудсманом з питань запобігання й усунення порушень законодавства про захист даних;
- контролювати загальний процес обробки даних.

Призначення відповідальної особи варто оформити відповідним наказом. Факт покладання на людину нових обов'язків потрібно закріпити документально — зазначити це у її трудовому договорі та посадових обов'язках (якщо такі передбачені), а також у Політиці щодо обробки персональних даних (Політиці приватності) тощо.

До обов'язків відповідальної особи доцільно віднести:

- контроль за проведенням заходів щодо захисту інформації;
- ведення обліку процесів обробки даних;
- ведення та підтримання в актуальному стані відповідної документації;
- здійснення внутрішнього контролю за дотриманням законодавства про захист даних;
- організацію проведення у колективі занять з даної тематики;
- організацію розгляду звернень (запитів) суб'єктів персональних даних, а також запитів третіх осіб чи Омбудсмана;
- участь у проведенні внутрішніх перевірок за фактами порушень вимог до обробки й захисту даних, а також інших інцидентів інформаційної безпеки;
- підготовку організації до перевірок з боку контролюючих органів (необхідних документів, інформації тощо);

Слід зауважити, що наведений перелік обов'язків не є вичерпним. У кожному окремому випадку для відповідальної особи необхідно визначити той обсяг повноважень та завдань, що дозволяє гарантувати належну обробку та захист даних в конкретній організації.

[16] Стаття 24 Закону «Про захист персональних даних»

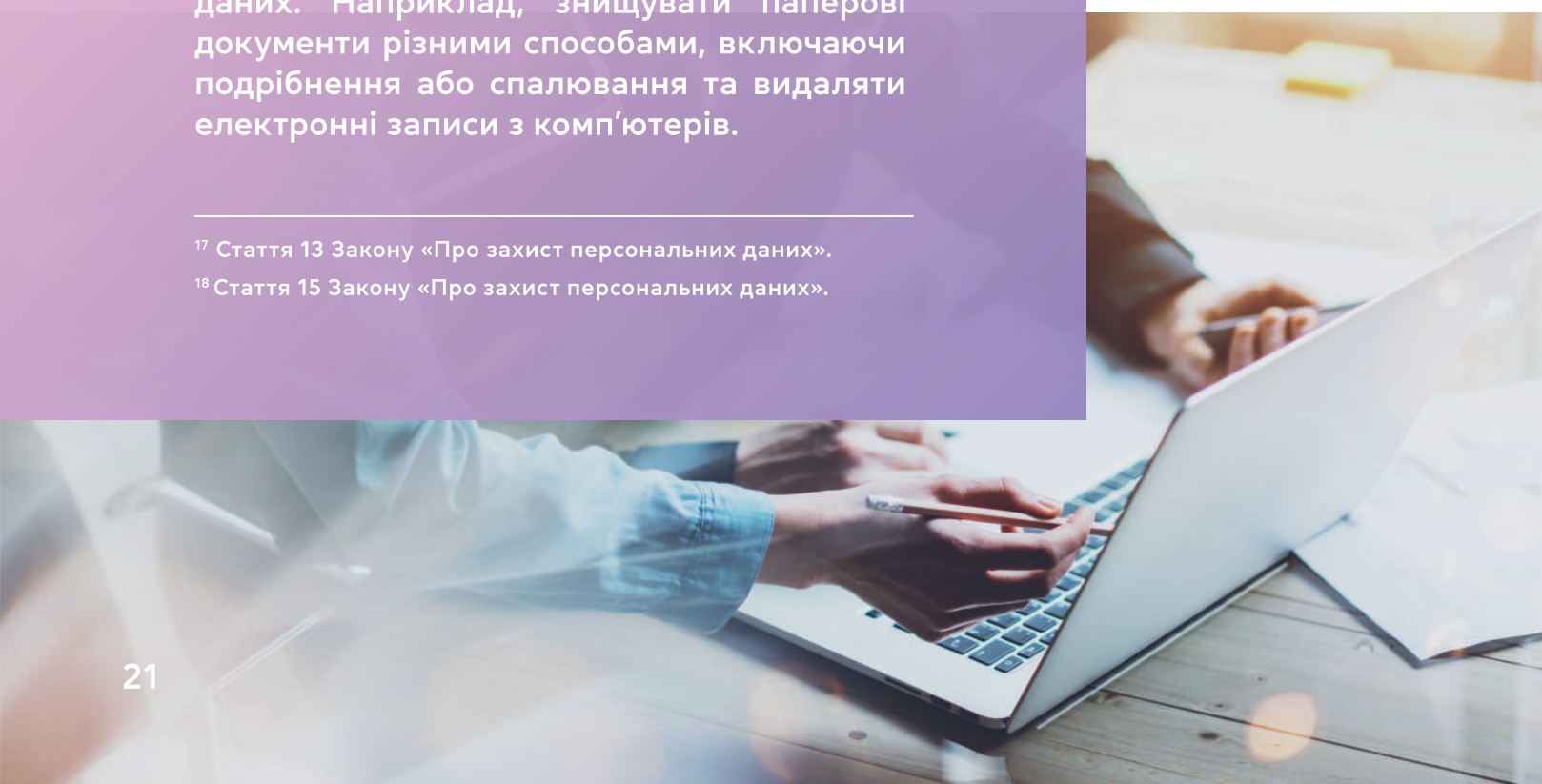
2.8. Встановити строк зберігання персональних даних

Під накопиченням персональних даних слід розуміти не лише формування бази файлів, а й весь комплекс дій з їх відбору, систематизації та подальшого зберігання[17]. Закон не встановлює конкретних строків зберігання інформації, тому потрібно самостійно його визначити та обґрунтувати.
Враховуючи принцип обробки даних «обмеження строку зберігання», зберігати інформацію потрібно не довше, ніж це необхідно для досягнення визначених цілей.
Наприклад, після завершення заходу потрібно видалити контакти учасників, якщо вони збиралися тільки для його організації. Подальше використання персональних даних для іншої мети можливе тільки за згодою суб'єктів персональних даних.

У Законі визначено[18], що персональні дані підлягають видаленню або знищенню у разі:
1. закінчення строку зберігання, встановленого законом або згодою особи, чиї дані збираються;
2. припинення правовідносин між суб'єктом персональних даних та володільцем чи розпорядником;
3. видання відповідного припису Уповноваженим Верховної Ради України з прав людини;
4. набрання законної сили рішення суду щодо видалення або знищення даних.

Хорошою практикою можна вважати, коли в організації є графік зберігання й видалення даних. Наприклад, знищувати паперові документи різними способами, включаючи подрібнення або спалювання та видаляти електронні записи з комп'ютерів.

[17] Стаття 13 Закону «Про захист персональних даних».
[18] Стаття 15 Закону «Про захист персональних даних».



ПРАВА

III. Забезпечення прав осіб, чиї дані збираються

01 Розробити процедури отримання згоди

02 Повідомляти про обробку особистих даних дітей

03 Забезпечити право на інформацію

04 Право на доступ до свої даних

05 Право на заперечення проти обробки даних

Культура поваги до приватного життя людини починається з розуміння, що людина має право на свої дані. Тому необхідно зробити певні кроки, аби подбати про права осіб, чиї дані збирає бо планує це робити.

3.1. Розробити процедури отримання згоди

У контексті роботи громадських організацій найбільш розповсюдженою підставою для обробки даних – є отримання згоди особи, чия інформація збирається. У попередніх розділах вже описали, які є види згод та як їх можна отримати. Суть у тому, навіть якщо організація отримала, наприклад, усну згоду, це також варто зафіксувати, щоб, у разі необхідності, мати доказ законної обробки даних. Отримання згоди — це, по суті, надання людині можливості контролювати потік інформації про себе. Такі дії з боку організації можуть зміцнити довіру до її діяльності.

Порядок отримання згоди особи, в тому числі у формі електронного документа, на збір і обробку її персональних даних, розробляється відповідно до діяльності організації. Скажімо, якщо це гугл-форма, тоді там має бути розміщено повідомлення про обробку даних, де людина, заповнюючи інформацію про себе, може зробити відмітку, що вона погоджується на збір даних. Організація повинна ознайомити особу, чиї дані збирає, про підстави та мету їх збору, а також з можливою передачею інформації третій стороні.

Згода суб'єкта на збір й обробку персональних даних має містити:

- прізвище та ім'я (або інші дані про суб'єкта персональних даних);
- найменування та адреса організації, що отримує згоду на обробку даних;
- вказівку на підставу й мету обробки даних;
- перелік даних, на обробку яких дається згода;
- перелік дій з персональними даними, на вчинення яких дається згода, включаючи можливість передачі їх третім особам;
- права осіб, чиї дані збираються (зокрема, право на заперечення);
- термін, протягом якого діє згода суб'єкта персональних даних.

3.2. Право на інформацію

Законом визначено[19], що особа має право на доступ до своїх даних. А також:

- знати про джерела збирання, місце знаходження своїх персональних даних, мету їх обробки;
- знати про умови надання доступу до даних, зокрема інформацію про третіх осіб, яким вони передаються;
- на доступ до своїх персональних даних;
- пред'являти вимогу із запереченням проти обробки своїх персональних даних;
- пред'являти вимогу щодо зміни або знищення своїх персональних даних, якщо вони обробляються незаконно чи є недостовірними;
- на захист своїх персональних даних від незаконної обробки та випадкової втрати, знищення, пошкодження у зв'язку з умисним приховуванням, ненаданням чи несвоєчасним їх наданням;
- на захист від надання відомостей, що є недостовірними чи ганьблять честь, гідність та ділову репутацію фізичної особи;
- вносити застереження стосовно обмеження права на обробку своїх даних під час надання згоди;
- відкликати згоду на обробку персональних даних;
- знати механізм автоматизованої обробки персональних даних;
- на захист від автоматизованого рішення, яке має для нього правові наслідки.

[19] Стаття 8 Закону «Про захист персональних даних».

3.3. Право на доступ до своїх даних

Як вже зазначено раніше, в організації має бути забезпечено механізм розгляду запитів про доступ до персональних даних та іншої довідкової інформації. Розгляд запитів відбувається протягом місяця з моменту його отримання.
Разом з тим, особа може звернутися з вимогою виправлення своїх персональних даних. Організація повинна забезпечити точність та актуальність інформації, яку обробляє, тому треба її регулярно переглядати та перевіряти.
У людини є право «на забуття», тому може звернутися з проханням видалити свої дані. А також, інформацію слід видаляти, коли вона більше не потрібна для тієї мети, для якої збиралася першочергово.

3.4. Право на заперечення проти обробки даних

Фізичні особи мають право заперечувати проти обробки своїх персональних даних, навіть якщо попередньо надавали на це згоду.
Наприклад, організації слід:
- інформувати людей, що вони мають на заперечення проти обробки своїх даних;
- впровадити процес, який дозволить людям подавати запит на заперечення (наприклад, написавши лист на електронну адресу);
- встановити правила запису будь-яких заперечень, які отримує організація в усній формі;
- мати процедури для розгляду заперечень проти обробки даних і запису результатів;
- інформувати людей про результат розгляду їхнього запиту на заперечення.

3.5. Повідомляти про обробку особистих даних дітей

Якщо організація пропонує послуги безпосередньо дітям, то потрібно інформувати про конфіденційність інформації у зрозумілій для дитини формі. Хорошою вважається практика, коли окрім прав, ще роз’яснюються потенційні ризики, пов'язані з обробкою їхніх даних. Будь-яка інформація, адресована дитині, повинна бути короткою, ясною і написаної простою мовою. Якщо послуги організації розраховані на дорослу аудиторію, то варто роз’яснити вікові обмеження.
Отже, інформування дитини про обробку її даних повинно здійснюватися:
- лаконічно, прозоро, чітко і легко доступно;
- написані ясною і зрозумілою мовою, зрозумілою дитині (відповідно до віку);
- пояснювати ризики, пов'язані з обробкою, і прийняті превентивні заходи;
- безоплатно.

БЕЗПЕК

IV. Безпека даних та внутрішній контроль

Якщо організація зберігає паперові та електронні записи, що містять персональні дані, тоді необхідні відповідні заходи безпеки. Потрібно уникати несанкціонованого доступу, знищення або зміни даних[20]. Для цього визначається власна політика безпеки інформації, яка поєднує заходи щодо запису, передачі, архівування, створення резервних копій, доступу, зберігання та знищення даних. Усі ці процедури (правила) повинні бути прописані у внутрішніх документах (положеннях, інструкціях тощо) та відповідати вимогам законодавства[21].
Важливо до початку роботи з даними обговорити у команді усі потенційні ризики. Це дасть можливість правильно сформувати необхідні заходи безпеки.

Наприклад, відповісти на питання:

- яким чином збирається інформація (можливі ризики)?
- де зберігається (можливі ризики)?
- хто має до неї доступ (можливі ризики)?
- хто несе відповідальність за безпеку?

4.1. Безпека даних

В організації повинні бути розроблені «правила» доступу до інформації. «Злам паролів» — поширена загроза, тому треба застосовувати надійні паролі. Наприклад, у момент введення, пароль не повинен відбиватися на екрані. Усі користувачі мають бути попереджені про відповідальність за розголошення конфіденційної інформації. Також слід встановлювати антивірусне програмне забезпечення на комп'ютери, де зберігаються дані. Періодично створювати резервні копії, щоб можна було відновити інформацію, у разі непередбачуваних обставин.

[20] Стаття 24 Закону «Про захист персональних даних».

[21] Про внутрішні документи зазначено у першому кроці.

КА КОНТ

4.2. Контроль за виконання законодавства у сфері захисту даних

Для впевненості у тому, що організація дотримується усіх положень законодавства, варто запровадити процедури внутрішнього контролю. Належна система контролю дозволяє отримати реальне уявлення про стан безпеки даних та сприяє своєчасному виявленню й усуненню порушень у цій сфері. Внутрішній контроль може здійснюватися керівництвом організації, окремою відповідальною особою або колегіальним органом (наприклад, комісією). Він повинен мати плановий характер, складатися у довільній формі та визначати: об'єкти контролю (процеси: збору, зберігання, передачі тощо); заходи проведення (внутрішня перевірка); способи, заходи та відповідальних осіб.

Наприклад, у плані проведення внутрішнього контролю доцільно передбачити заходи, що дозволяють перевірити:

- види та категорії персональних даних, що обробляються;
- правові підстави обробки;
- законність реальних цілей обробки та їх відповідність офіційно проголошеним;
- загальний стан дотримання прав суб'єктів персональних даних;
- внутрішню документацію, яка врегульовує процеси обробки даних;
- критерії, за якими здійснюється доступ персоналу до персональних даних;
- дотримання правил інформаційної безпеки;
- технічні ресурси та програми, які використовуються у процесах обробки;
- порядок фіксації інцидентів безпеки при обробці персональних даних;
- повідомлення Омбудсмана у разі обробки чутливої категорії даних;
- дотримання вимог законодавства під час надання відповідей на звернення суб'єктів персональних даних та третіх осіб;
- порядок поширення та/або передачі персональних даних третім особам;
- терміни зберігання даних;
- порядок видалення та знищення даних.

Інструменти для здійснення внутрішнього контролю, які можна використовувати:

- опитування та співбесіди з персоналом;
- перевірка обладнання та програмного забезпечення, де зберігається інформація;
- перевірка внутрішньої документації.

За результатами перевірки варто готувати відповідний звіт, у якому зазначаються:

- вид перевірки (планова/позапланова), підстави та цілі її проведення;
- перелік проведених під час перевірки заходів;
- опис встановлених порушень та недоліків, стислий аналіз причин їх наявності;
- висновок про стан безпеки даних та рекомендації з усунення виявлених недоліків.

ДОДАТО

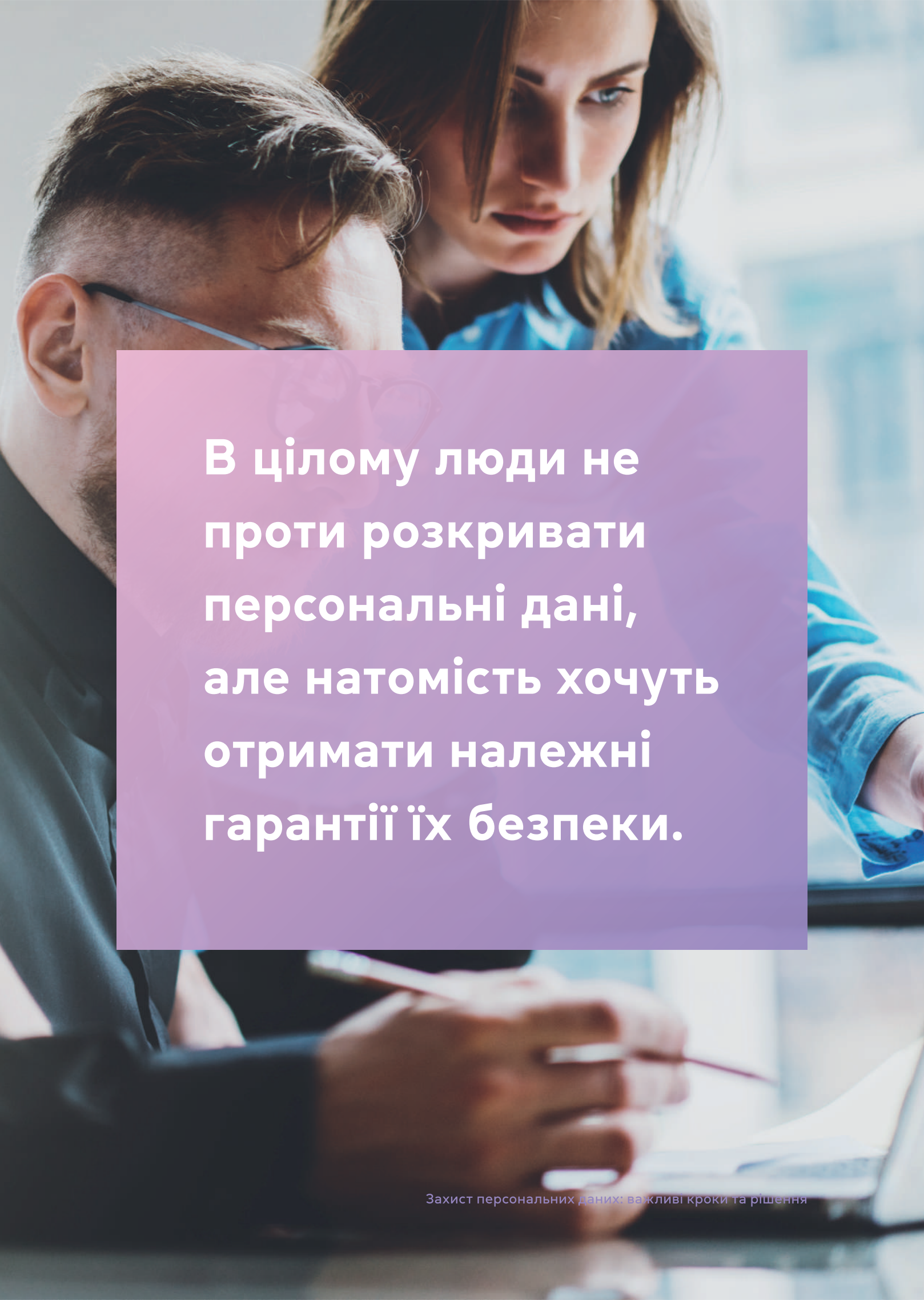
Додаток 1: **Джерела правового регулювання захисту персональних даних** (не вичерпний перелік)

1. Стаття 32 Конституції України.
2. Стаття 12 Загальної декларації прав людини.
3. Стаття 17 Міжнародного Пакту про громадянські і політичні права, ратифікованого Указом Президії Верховної Ради УРСР No2148-VIII (2148-08) 1973 року).
4. Стаття 8 Конвенції про захист прав людини і основоположних свобод.
5. Конвенція Ради Європи про захист осіб у зв'язку автоматизованою обробкою персональних даних.
6. Директива No2002/58/ЄС Європейського Парламенту і Ради ЄС «Про обробку персональних даних та захист таємниці сектора електронних комунікацій».
7. Директива No95/46/ЄС Європейського Парламенту і Ради ЄС «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 року.
8. Закон України «Про захист персональних даних».
9. Стаття 188—39 «Порушення законодавства у сфері захисту персональних даних» та стаття 188—40 «Невиконання законних вимог Уповноваженого Верховної Ради України з прав людини» Кодексу України про адміністративні правопорушення.
9. Стаття 182 «Порушення недоторканності приватного життя» Кримінального кодексу України.
10. Типовий порядок обробки персональних даних, затверджений наказом Уповноваженого Верховної Ради України з прав людини «Про затвердження документів у сфері захисту персональних даних» від 08.01.2014 No1/02-14.
11. Порядок здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних.
12. Порядок повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних при їх обробці, а також оприлюднення вказаної інформації.
13. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент захисту даних (GDPR/ Регламент),

ПОСИЛА

Корисні посилання:

1. «Цифрова освіта», Національна кампанія з цифрової грамотності від Міністерства цифрової трансформації України: https://thedigital.gov.ua/projects/osvita.
2. Повідомлення про обробку персональних даних (форма заяв): https://ombudsman.gov.ua/ua/page/zpd/povidomlennya/.
3. Оприлюднення інформації на виконання статті 9 Закону України «Про захист персональних даних»: https://ombudsman.gov.ua/ua/page/zpd/obnarodovanie-informatsii/.
4. Політика захисту персональних даних УВКБ ООН: https://www.refworld.org/cgi-bin/texis/vtx/rwmain/opendocpdf.pdf?docid=5be2baf44.
5. Посібник з європейського права у сфері захисту персональних даних: https://www.echr.com.ua/wp-content/uploads/2018/02/Handbook_data_protection_UKR.pdf.
6. Актуальні рішення Європейського суду з прав людини у контексті застосування статті 8 Конвенції про захист прав людини і основоположних свобод: https://ombudsman.gov.ua/ua/all-news/pr/aktualni-rishennya-yevropejskogo-sudu-z-prav-lyudini-u-kontekst i-zastosuvannya-statti-8-konvencziї/.
7. Роз'яснення щодо доступу до персональних даних за адвокатськими запитами: https://ombudsman.gov.ua/ua/all-news/pr/shhodo-dostupu-do-person alnix-danix-za-advokatskimi-zapitami/
8. Навчальний курс «Як захистити персональні дані» від Офісу Омбудсмана та Офіс Ради Європи в Україні: https://www.coe.int/uk/web/kyiv/-/ak-zahistiti-personal-ni-dani-ofis-ombudsmana-ta-ofis-radi-evropi-v-ukraini-zapuskaut-navcal-nu-iniciativu



В цілому люди не проти розкривати персональні дані, але натомість хочуть отримати належні гарантії їх безпеки.





The Tenth of April
Громадська організація «Десяте квітня»

м. Одеса
вул. Героїв Крут, 15, (був. Терешкової), 5 поверх
Тел.: +38 (048) 766-00-04
Тел.: +38 (098) 393-86-03, +38 (050) 979-93-87
Електронна пошта: **idps@dk.od.ua**

м. Херсон
проспект Ушакова, буд. 25, офіс №618
Тел.: +38 (095) 204-99-78
Тел.: +38 (095) 434-57-58, +38 (095) 809-95-07
www.dk.od.ua

UNHCR Агентство ООН у справах біженців

Цю публікацію було підготовлено за підтримки Агентства ООН у справах біженців (UNHCR). Зміст цієї публікації є виключно відповідальністю ГО «ДЕСЯТЕ КВІТНЯ» і не може використовуватися для відображення точки зору Агентства.