Симфонії захисту персональних даних: на сцені гуманітарні організації

Симфонії захисту персональних даних: на сцені гуманітарні організації

Тетяна Авдєєва

Київ 2023

Аналітичне дослідження «Симфонії захисту персональних даних: на сцені гуманітарні організації»

Метою дослідження є аналіз практик роботи з персональними даними організацій, які виконують гуманітарні функції в межах збройного конфлікту (російської агресії в Україні), оцінювання потенційних ризиків політик і практик таких організацій та можливі рішення для посилення захисту даних в умовах війни.

Загальна редакція: Тетяна Авдєєва
Авторський колектив: Тетяна Авдєєва
Літературна редакція: Мар'яна Добоні
Дизайн/верстка: Інна Смучок

Дослідження «Симфонії захисту персональних даних: на сцені гуманітарні організації» зроблено в рамках проєкту «Документування воєнних злочинів вчинених РФ» за фінансової підтримки НЕД, США (National Endowment for Democracy, USA). Погляди авторів дослідження не обов'язково відображають офіційну позицію NED та Уряду США.

Симфонії захисту персональних даних: на сцені гуманітарні організації
Аналітичне дослідження/За заг. ред. Авдєєвої Т.С. – Київ, 2023 р. – 54 с.

ЗМІСТ

ВСТУП 7

РОЗДІЛ I.
Режим воєнного стану грає першу скрипку 10

РОЗДІЛ II.
Оркестр міжнародних стандартів 14

РОЗДІЛ III.
Композиції захисту даних по-українськи 24

РОЗДІЛ IV.
Чи потрапляють гуманітарні організації в такт зі стандартами? 30

РОЗДІЛ V.
Рекомендації 48

ВСТУП

Війна — найбільша загроза для права на життя та здоров'я, а у випадку російського вторгнення — ще й для права не бути об'єктом тортур. На тлі таких фундаментальних речей усе інше стає менш важливим. До прикладу, хто буде перейматися через неможливість вийти на протест, провести релігійний обряд або написати допис про те, що відбувається за вікном, якщо над головою літають ракети? Проте насправді є речі, які, хоч і непрямо, але достатньо суттєво впливають на безпеку. Серед них одне з ключових питань — захист персональних даних. Так, витоки даних можуть призвести до переслідування вразливих груп, затримання активістів і навіть масових розстрілів тих, хто афілійований з державними структурами (як це неодноразово відбувалося на окупованих Росією територіях).

Під час збройних конфліктів персональні дані відіграють надзвичайно важливу роль як для захисту цивільного населення (як-от надання гуманітарної допомоги), так і планування операцій, прогнозування розвитку воєнних дій (складання дорожньої мапи потреб) та екстрених комунікацій (зв'язку з родичами або організаціями, що забезпечують евакуацію тощо). Загалом дослідження показують, що під час міжнародного збройного конфлікту найчастіше використовують такі джерела чутливої інформації:

- **дані розвідки або стеження,** які переважно надають загальне розуміння тенденцій у переміщеннях осіб (якщо при цьому не застосовуються спеціальні технології біометричної ідентифікації, які забезпечують ширший спектр можливостей органам, які збирають такі дані);

- **відкриті дані,** що містяться в соціальних мережах (наприклад, за моделлю дії сумнозвісного Clearview AI), блогах і медіа (відповіді на інтерв'ю, цільові дослідження тощо). Така інформація, хоч і є доступною, допомагає, до прикладу, поширювати ворожу пропаганду, адже сприяє кращому вивченню аудиторії або дозволяє ідентифікувати затриманих осіб;

- інформація, що надається у **відповідь на опитування, у SMS, на гарячих лініях** тощо. Такі дані використовуються для прогнозування потреб і рідко можуть допомогти ідентифікувати особу (адже цілі збору таких даних дещо інші). Утім, з огляду на те, що технічно дані все одно зберігаються, існують ризики їх витоку або потрапляння до сторін, які воюють;

- **інформація, надана самими особами при отриманні гуманітарної допомоги** (джерело найбільшої кількості зібраних даних). Така інформація може містити як обов'язкові дані, так і так звані залишкові дані, які можна використати для профайлінгу або відстеження особи. Саме тому з такими даними слід поводитися надзвичайно обачно.

У відповідь на таку масштабну обробку персональних даних з різних джерел ще у 2017 році Міжнародний комітет Червоного Хреста (далі — МКЧХ) наголосив на потребі посилити захист для месенджерів і соціальних мереж, а у 2018 році — підкреслив, що спеціальних правил захисту даних потребують додатки для онлайн-платежів. Згодом, у 2019 році, МКЧХ напрацював Політику обробки біометричних даних, що містить рекомендації, як забезпечити нейтральність, неупередженість і незалежність при обробці даних цивільних під час збройного конфлікту. Зрештою, у 2021 році вийшов оновлений Довідник щодо захисту даних під час гуманітарних акцій, покликаний дати відповідь, якщо не на всі, то на більшість актуальних викликів у сфері захисту чутливої інформації. Усі згадані документи кваліфікували витоки даних, їх недбалу обробку й зберігання як основні виклики, з якими наразі стикаються і організації, і користувачі. Трохи згодом ми з'ясуємо, чи ці рекомендації відповідають реаліям, у яких працюють надавачі гуманітарної допомоги під час сучасних збройних конфліктів.

Проте, як показує практика, найчастіше персональні дані використовують для надання гуманітарної допомоги: одноразової або регулярної фінансової підтримки, забезпечення

певними ліками або речами першої потреби, надання статусу біженця, особи, яка потребує тимчасового захисту, надання тимчасового притулку тощо. Тому саме ця сфера вимагає найбільш прискіпливого аналізу. Міжнародні організації, зокрема, збирають і зберігають персональні дані переміщених осіб, щоб допомоги відновити зв'язки з рідними після завершення збройного конфлікту. Така практика не нова і вже застосовувалася під час конфлікту в Південному Судані та після епідемії еболи в Демократичній Республіці Конго.

Велику кількість даних збирають і постійні надавачі гуманітарної допомоги, зокрема для прогнозування витрат. Наприклад, Шведська агенція з міграції аналізує «великі дані», щоб встановити кількість мігрантів або шукачів притулку. Утім, разом зі зберіганням даних проблемною стала їх репрезентація: іноді не всі особи можуть отримати допомогу через брак інформації про потрібні медикаменти, харчі чи грошові кошти. Ця проблема стосується не самого факту збору даних, а їх передачі між різними організаціями місцевого, регіонального та міжнародного рівнів.

Щоб уникнути таких ситуацій або хоча б зменшити типові ризики, міжнародні та регіональні організації, чиєю постійною функцією є надання гуманітарної допомоги, напрацювали низку рекомендацій щодо правильного поводження з персональними даними під час збройних конфліктів. Хоч переважно вони досить загальні, проте слугують чудовим меппінгом викликів, ризиків і слабких місць політик захисту даних, які виникають на практиці. Такі правозахисні органи, як Спеціальний доповідач ООН із захисту права на приватність, зазначають, що слід контекстуалізувати всі ризики. Так, хоч гуманітарні організації і запевняють, що вони зібрані дані анонімізують, завжди існує можливість повторної ідентифікації особи за допомогою поєднання кількох баз даних. А тому, окрім декларативних стандартів, слід зважати ще й на практичні виклики, які постають з розвитком технологій і переходом збройних конфліктів на новий рівень. Адже, намагаючись надати допомогу, організації часом можуть нашкодити ледве не більше, залишаючи людей цілями переслідувань, дозволяючи використовувати їхні дані для маніпуляцій, планування воєнних операцій чи інформаційних атак.

Повномасштабне вторгнення Росії в лютому 2022 року спричинило значну потребу в гуманітарній допомозі для внутрішньо переміщених осіб (далі — ВПО), дітей, що втратили батьків/опікунів унаслідок збройної агресії, вразливих верств населення та багатьох інших категорій українців. Для уникнення зловживань і рівномірного розподілу доступної допомоги органи державної влади і місцевого самоврядування, як і міжнародні та національні гуманітарні організації, вимушені фіксувати особу тих, кому таку допомогу надають.

Будь-які записи, що дозволяють ідентифікувати особу, автоматично передбачають збір персональних даних і їх обробку. Правила роботи з конфіденційною інформацією передбачені як міжнародними актами (жорсткого і м'якого права), так і національним регулюванням (Законом України «Про захист персональних даних», роз'ясненнями Уповноваженого Верховної Ради України з прав людини щодо захисту даних під час воєнного стану тощо). Відповідно до Закону України «Про гуманітарну допомогу», організації, які її надають, самостійно визначають обсяг персональних даних, мету, умови й строки їх обробки та способу захисту. Також покладені законом обов'язки включають створення бази персональних даних набувачів і правил доступу до них й обробки даних у такій базі, обрання особи, яка буде здійснювати нагляд за такими процесами тощо.

Здавалося б, що може піти не так за наявності деталізованих керівництв? Проте навіть це не врятувало український інформаційний простір від скандалів: наприклад, Дитячий фонд ООН (далі — ЮНІСЕФ) звинувачували в незаконному й непропорційному зборі даних українців, які отримували грошову допомогу від організації (порушенні принципу отримання згоди). Варто наголосити, що звинувачення згодом спростувала команда фактчекерів «Вокс Україна», які довели, що жодних порушень з боку міжнародної організації в питанні захисту персональних даних немає.

Водночас цей випадок привернув суспільну і, що головніше, правозахисницьку увагу

до питання обмеження і захисту приватності в період дії воєнного стану. Зокрема, серед актуальних проблем як юридична, так і технічна спроможність організацій, які надають допомогу вразливим верствам населення, захистити зібрані персональні дані й забезпечити їх недоступність для країни-агресора, у тому числі і в окупованих регіонах. З огляду на різке зростання кількості гуманітарних організацій з 24 лютого 2022 року (у п'ять разів порівняно із ситуацією до повномасштабного вторгнення) виникає занепокоєння щодо наявності в новостворених організацій адекватних політик щодо обробки даних, у тому числі й чутливої інформації. Так, у 2022 році фокус переважно робився на самому наданні допомоги, а дотримання процедур захисту даних, їх належне зберігання — відійшли на другий план. У цьому контексті, наприклад, актуальне питання, чи міжнародні організації, як-от ЮНІСЕФ, Всесвітня продовольча програма та МКЧХ, поширюють зібрані дані серед своїх осередків у країні-агресорі (надають доступ до загальної бази даних).

Щоб відповісти на ці й багато інших питань, пов'язаних зі збором персональних даних гуманітарними організаціями, УМДПЛ провела комплексне дослідження стану дотримання національних і міжнародних стандартів. **Метою дослідження** став аналіз практик роботи з персональними даними організацій, які виконують гуманітарні функції в межах збройного конфлікту (російської агресії в Україні), оцінювання потенційних ризиків політик і практик таких організацій та можливі рішення для посилення захисту даних в умовах війни.

Ключові завдання аналітичного дослідження передбачали:

- збір інформації про чинні політики захисту персональних даних організаціями, які виконують гуманітарні функції в контексті війни в Україні;
- виявлення небезпечних або неправомірних практик збору, обробки, зберігання чи передачі персональних даних у межах надання гуманітарної допомоги;
- оцінювання ризиковості таких практик і пропонування юридичних і технічних варіантів розв'язання проблеми недостатнього захисту персональних даних.

У межах дослідження автори послуговувалися **даними** з відкритих джерел інформації, вивчивши, зокрема, практику міжнародних і національних судів, статистичними даними на вебсайтах організацій, результатами соціальних опитувань та індексів дотримання правил захисту даних, цільовими інтерв'ю й опитуваннями, матеріалами всеукраїнських і регіональних медіа, дослідженнями правозахисних організацій, а також відповідями на інформаційні запити від національних і міжнародних організацій та експертів. Якщо нам доводилося використовувати матеріали з неофіційних джерел, то ми проводили перехресну перевірку правильності інформації в інших джерелах; також у тексті згадано про відсутність підтвердження даних, якщо вони були наявні лише в одному джерелі / кількох джерелах, які з певних причин не можна вважати надійними або об'єктивними.

У результаті дослідження було розроблено рекомендації для міжнародних, іноземних та українських організацій щодо покращення політик захисту персональних даних при наданні гуманітарної допомоги та виконанні інших гуманітарних функцій. Також надано низку рекомендацій іншим стейкхолдерам, які впливають на захист та передачу персональних даних при наданні гуманітарної допомоги відповідними організаціями (як-от держава, органи місцевого самоврядування, особи, які отримують допомогу etc).

РОЗДІЛ І.
Режим воєнного стану грає першу скрипку

Безсумнівно, збройний конфлікт є відхиленням від звичного порядку захисту, обмежень і реалізації прав людини. Війна породжує нові ризики, які часто зміщують акценти в балансуванні прав. Так, актуальнішим стає захист права на життя (адже збільшується кількість загроз), а от право на свободу мирних зібрань, право на свободу переміщення чи виборчі права зазнають більших обмежень. Така зміна парадигми й пріоритетів під час збройного конфлікту зафіксована в міжнародному й національному праві. Зокрема, держава має право відступати від зобов'язань за міжнародними договорами в разі виникнення надзвичайних ситуацій (природних лих або техногенних катастроф, епідемій, суспільних заворушень тощо) або початку війни. Підставою для цього є рішення про введення відповідно надзвичайного або воєнного стану, ухвалене на національному рівні.

Такі особливі правові режими дозволяють національним органам влади ефективніше захищати основоположні права й балансувати інтереси залежно від нагальних потреб і ризиків, про які найкраще обізнані (знову ж таки) національні уряди. По суті, обидва режими передбачають розширення дискреції держави й можливість ухвалювати певні рішення, не передбачені законодавством, яке застосовується в мирні періоди. Утім, така дискреція не абсолютна: міжнародне право й національні законодавства містять запобіжники від можливих зловживань, зокрема, щоб уникнути перетворення режимів на авторитарні. Саме тому, перш ніж оцінити, чи дотримуються гуманітарні організації правил захисту персональних даних, варто з'ясувати, а які ж саме правила застосовні як на рівні держави, так і приватних акторів.

Міжнародні стандарти й режим відступу від зобов'язань. Можливість (чи заборона) відступати від зобов'язань за міжнародними конвенціями передбачена окремо кожним договором. У контексті російської агресії актуальні два документи, ратифіковані Україною, — Міжнародний пакт про захист громадянських і політичних прав (далі — МПГПП) і Європейська конвенція з прав людини (далі — ЄКПЛ). Кожен з них має окремий механізм для активування режиму відступу від зобов'язань у разі виникнення надзвичайних обставин, а також стандарти, яких слід дотримуватися при впровадженні додаткових обмежень на період такого режиму. З'ясуємо, у чому полягають їхні особливості.

Стаття 4 МПГПП передбачає механізм відступу від зобов'язань за Пактом у разі виникнення надзвичайних обставин, за яких «життя нації перебуває під загрозою і про наявність якого офіційно оголошується». Хоча це формулювання досить розмите, стаття 4 встановлює декілька критеріїв дійсності та правомірності відступу (які, утім, усе ж загальні й нечіткі).

Умови, за яких відступ від зобов'язань за статтею 4 Пакту дійсний:

- надзвичайне становище, за якого життя нації перебуває під загрозою;
- відступ здійснено в тих межах, «яких вимагає гострота становища»;
- відступ сумісний з іншими зобов'язаннями за міжнародним правом;
- відступ не призводить до дискримінації лише на основі раси, релігії, кольору шкіри, статі, мови чи соціального походження;
- відступ не стосується права на життя, права не бути об'єктом тортур, права на захист від рабства, права не мати обмеження волі через неможливість виконати
- зобов'язання, права не бути покараним без закону та права на свободу думки, совісті і релігії;
- держава вчасно і в повному обсязі поінформувала Генерального секретаря ООН про вжиті заходи і їх причини.

Положення статті 4 протлумачені в Загальному коментарі № 29 до МПГПП. Так, Комітет ООН з прав людини підкреслює, що відступи від зобов'язань мають тимчасовий характер і є винятковими за своєю природою [§ 2]. Зокрема, це означає, що держава не здатна розв'язати проблему захисту основоположних прав чи інтересів за допомогою вже чинних законів. Також Комітет наголосив, що при формулюванні відступу держава має чітко перелічити можливі додаткові заходи та обґрунтувати необхідність кожного з них для захисту легітимного інтересу. Інакше вона порушуватиме принципи необхідності та пропорційності. Коментар також містить додатковий обов'язок для держави (який не згадано в статті 4 напряму) — відновлювати порушені права чи відшкодовувати шкоду.

Оскільки МПГПП поширюється на дещо більшу кількість країн, ніж ЄКПЛ (про яку ми поговоримо трохи згодом), кількість відступів за всю історію дії Пакту доволі значна. Лише за 2020 рік у відповідь на пандемію Генеральний секретар ООН отримав 27 повідомлень про відступ від зобов'язань. Через хвилю відступів Комітет ООН з прав людини видав заяву із закликом не відступати від зобов'язань у випадках, де можливо захистити права і свободи, вдаючись до звичайного механізму обмежень за основними статтями Пакту. Окрім того, повідомлення про відступи від більшості країн були оцінені як дуже розмиті й нечіткі, з браком належного обґрунтування додаткових обмежень прав.

Система, передбачена ЄКПЛ, дещо інша: стаття 15 встановлює не тільки чіткий механізм відступу від зобов'язань під час надзвичайної ситуації, але й певні умови його дійсності. На відміну від МПГПП, Конвенція безпосередньо згадує війну як підставу для розширення державної дискреції й зміну призми, крізь яку оцінюють права людини. Окрім того, вона передбачає й деякі інші вимоги.

Умови, за яких відступ від зобов'язань за статтею 15 Конвенції дійсний:

- наявність війни або іншої суспільної небезпеки, яка загрожує життю нації;
- відступ не стосується права на життя (окрім випадків смерті через правомірні воєнні дії), права на заборону тортур і рабства, права не бути покараним без закону;
- відступ здійснено в тих межах, «яких вимагає гострота становища»;
- держава вчасно і в повному обсязі поінформувала Генерального секретаря Ради Європи про вжиті заходи і їх причини.

Формальне виконання вимог не «розв'язує руки» держави в питанні обмеження прав. Хоча статтю 15 ЄКПЛ нечасто використовували раніше (це робили лише декілька країн), після початку пандемії багато країн почали звертатися до цього механізму. І це породило досить широку практику в інтерпретації положень статті 15, а також визначення меж такої державної дискреції Європейським судом з прав людини (далі — ЄСПЛ), зокрема і щодо обмеження права на приватність і захист персональних даних.

Важливо, що до 24 лютого 2022 року жодна держава **не відступала від зобов'язань на підставі стану війни.** Це означає, що порівняння з іншими прецедентами слід робити дуже обачно, адже ані пандемія, ані суспільні заворушення, ані ймовірні терористичні акти за рівнем інтенсивності й небезпеки не зрівняються зі збройним конфліктом. Тому, аналізуючи практику ЄСПЛ, слід зважати скоріше на загальні принципи тлумачення статті 15, ніж проводити конкретні паралелі з обставинами справ.

Перш за все ЄСПЛ вважає режим відступу від зобов'язань винятковим механізмом. У справі «Ireland v the United Kingdom» Суд наголосив, що спершу оцінює відповідність обмеження основним положенням ЄКПЛ, і лише коли встановлено невідповідність, аналізує, чи відступ від зобов'язань був належним [§ 191]. З цього можна зробити логічний висновок: не кожен відступ від зобов'язань може бути необхідним і пропорційним, навіть якщо формальні вимоги про повідомлення чи наявність суспільної небезпеки існують.

Оцінюючи необхідність і пропорційність, Суд зважає на такі критерії:

- достатність звичайних законів для захисту легітимного інтересу;
- здатність заходів зарадити в надзвичайній ситуації (захистити певний інтерес);
- чіткість і передбачуваність відступів від зобов'язань, конкретний перелік заходів, можливих для застосування на такий період;
- перегляд відступу від зобов'язань з плином часу;
- послаблення заходів із часом або в певних регіонах;
- наявність запобіжників від зловживань;
- інші критерії, які залежать від природи обмеженого права.

Хоча валідність повідомлення про відступ Суд оцінює вже тоді, коли виникає прецедент (коли до ЄСПЛ надходить скарга), держави теж мають зважати на ці критерії при формулюванні відступів від зобов'язань і визначенні їх обсягу. Зокрема, як випливає зі справи «A. and Others v the United Kingdom», обмеження повинні бути правомірними саме на момент їх впровадження, проте мають враховувати й подальший розвиток подій, як-от зменшення інтенсивності заворушень тощо [§ 177].

Оцінювання необхідності й пропорційності ніколи не було простою справою, про що науковці зазначали ще від початку XXI століття, оцінюючи справи проти Сполученого Королівства, Греції й Туреччини. Утім, державі важливо від початку встановити передбачуваний правовий режим, щоб уникнути зайвих судових позовів як від власних громадян, так і іноземців, на яких такі обмеження впливають. Це актуально і у випадку України, тож варто проаналізувати обмеження, згадані в комунікації відступів від ЄКПЛ і МПГПП (їх надсилали одним документом).

Після початку повномасштабного вторгнення Україна надіслала повідомлення **про відступ від зобов'язань** за ЄКПЛ і МПГПП. Повідомлення надійшло 28 лютого і було зареєстроване Генеральним секретарем ООН

1 березня 2022 року. Згодом, 4 березня 2022 року, постійне представництво України надіслало доповнення до повідомлення, у якому було розтлумачено обсяг відступу від зобов'язань.

Саме повідомлення містить посилання на президентський указ про введення воєнного стану та закон, яким його було затверджено. Також у повідомленні міститься перелік конституційних прав, обмеження яких передбачено на період дії воєнного стану, і статей-відповідників МПГПП і ЄКПЛ. Після переліку йде майже дослівний переклад указу з можливими формами обмежень згаданих прав. Обґрунтувань, чому саме такі форми обмежень заплановано застосовувати, утім, держава не надала. На відміну від повідомлень багатьох держав під час пандемії чи суспільних заворушень, Україна не вказала чітких обмежень щодо деяких прав (як-от свободи вираження чи приватності), зазначивши в загальних рисах можливість їх обмеження. Згодом брак обґрунтувань зауважили у своєму дослідженні й експерти Ради Європи, які оцінювали правомірність відступу від зобов'язань.

Утім, припустімо, що посилання в самому повідомленні на законодавство про воєнний стан та акти національної влади достатньо. У такому разі всі дороги ведуть до указу Президента України про введення воєнного стану та супровідних актів уряду, тож саме час з'ясувати, наскільки ці документи чіткі та передбачувані.

Режим воєнного стану в українському законодавстві. Стаття 64 Конституції України передбачає можливість обмеження деяких прав в умовах воєнного або надзвичайного стану. Порядок введення воєнного стану та його особливості регулюються Законом України «Про правовий режим воєнного стану». Серед можливих заходів, які стосуються права на приватність, стаття 8 передбачає можливість перевірки документів, речей і житла, а також дозволяє реалізувати «інші заходи, передбачені нормами міжнародного гуманітарного права», які часом також стосуються передачі персональних даних. В іншому ж Закон надає загальну рамку, а специфічні обмеження мали б встановлювати безпосередньо акти, якими воєнний стан запроваджується.

24 лютого 2022 року, після початку повномасштабного вторгнення, на підставі пропозиції Ради національної безпеки і оборони України Президент видав указ «Про введення воєнного стану в Україні». Відповідно до указу Кабінет Міністрів України мав розробити план забезпечення й запровадження заходів воєнного стану. Після затвердження указу відповідним законом уряд розробив такий план, але щодо прав людини в ньому було лише декілька рядків, ще менше з них стосувалися приватності. Так, план дій просто продублював положення закону про воєнний стан, уповноваживши органи правопорядку та військові органи здійснювати перевірку документів осіб, а в разі потреби — огляд речей, транспортних засобів, багажу та вантажів, службових приміщень і житла громадян. Водночас стаття 25 Закону України «Про захист персональних даних» вказує, що відступи від положень статей про обробку даних можуть здійснюватися, лише якщо вони прямо передбачені іншими законодавчими актами. Якщо ж такі обмеження не були «активовані» у встановленому законом порядку, застосовним буде загальний режим обробки персональних даних.

Чи запроваджені спеціальні обмеження щодо права на захист персональних даних? На рівні президентського указу чи плану дій, розробленого урядом, — ні, звісно ж, окрім можливості перевіряти документи особи, її особисті речі й житло. Це означає, що обмеження права на приватність, які виходять за межі таких заходів мають бути передбачені законами й послуговуватися загальними вимогами Закону України «Про захист персональних даних». Ці регуляторні акти ми оцінимо, коли аналізуватимемо правила, за якими надається гуманітарна допомога та відбувається передача даних.

Якщо режим відступу від зобов'язань перш за все стосується держави, її дискреції й обов'язків обґрунтовувати обмеження, то чому ж важливо говорити про це, аналізуючи діяльність гуманітарних організацій?

- По-перше, відступ — це не лише можливість держави додатково обмежити права і зобов'язання пояснити, чому такі обмеження впроваджено, **а й спеціальний правовий режим на певній території.** Він застосовний до всіх суб'єктів, що діють у такому правовому полі, і накладає обмеження навіть на тих, щодо кого їх не очікують. Наприклад, часом гуманітарні організації можуть бути вимушені розкривати дані отримувачів допомоги за спрощеною процедурою на запит органів правопорядку якщо є підозра в порушенні закону. Утім, як помітно з аналізу запроваджених обмежень, таких вимог в Україні немає.

- По-друге, **спрощені правила часом запроваджують і для гуманітарних організацій,** адже їхня діяльність набуває більшої актуальності у кризові періоди, такі як війна чи природні лиха. У таких випадках, вони можуть збирати більш (чи навпаки) менше даних, що матиме вплив на права отримувачів допомоги.

Проте відступ від зобов'язань і режим воєнного стану є лише загальною рамкою. Окрім них, існує цілий масив міжнародних і національних стандартів, застосовних до гуманітарних організацій та отримувачів гуманітарної допомоги. Перш ніж аналізувати політики й практики діяльності таких організацій в Україні з'ясуємо, які стандарти розробили передові міжнародні органи.

РОЗДІЛ ІІ.
Оркестр міжнародних стандартів

Говорячи про міжнародні стандарти захисту персональних даних, європейські експерти найчастіше згадують два документи — Загальний регламент про захист даних (далі — GDPR), який діє на рівні ЄС і застосовний до компаній, що потрапляють під юрисдикцію ЄС, і Конвенцію про захист осіб у зв'язку з автоматизованою обробкою даних (далі — Конвенція 108+), яка застосовна до сторін, які її ратифікували (переважно держави-члени Ради Європи). Обидва документи стосуються загальних стандартів у сфері захисту даних, орієнтованих переважно на мирний час. Спеціальних положень про обробку даних під час надзвичайного стану майже немає, утім, саме на це рамкове регулювання обробки даних посилаються у всіх спеціальних рекомендаціях для гуманітарних організацій. Тож перш ніж розглядати точкові керівництва, з'ясуємо загальні стандарти у сфері захисту даних.

Конвенція 108+. Цей документ досить загальний і певною мірою застарілий порівняно із GDPR. Так, сама Конвенція набула чинності ще в 1981 році, а останні оновлення — Додатковий протокол — були підписані у 2001 році. Тобто більшість сучасних способів обробки даних, у тому числі і за допомогою систем, керованих штучним інтелектом, не враховано в положеннях цього акта. Проте, безперечно, релевантними у сфері обробки даних у гуманітарних цілях є такі принципи:

- законність збору та обробки даних;
- відповідність обробки даних цілям і меті їх збору;
- принцип мінімізації (ненадмірності) збору даних стосовно цілей їх обробки;
- точність і вчасне оновлення застарілих даних;
- обмеженість строків зберігання метою обробки даних.

Саме Конвенція 108+ заклала ці засади обробки персональних даних поряд з іншими важливими принципами, як-от безпека даних у юридичній та технічній площині, гарантії для суб'єкта персональних даних (повідомлення про факт обробки даних, можливість видалення чи виправлення даних, використання засобів правового захисту в суперечливих випадках тощо). Окрім того, Конвенція 108+ встановила ще одне важливе правило — існування особливої категорії даних (чутливих даних).

> Персональні дані про расову приналежність, політичні, релігійні чи інші переконання, дані, які стосуються здоров'я чи статевого життя, не можуть піддаватися автоматизованій обробці, якщо законодавство не забезпечує відповідних гарантій. Тобто такі дані є **чутливими.**

Важливо, що Додатковий протокол встановлює **обов'язок створити наглядові органи,** які стежитимуть за дотриманням правил обробки і захисту персональних даних. Хоча деталізованих вимог до такого наглядового органу немає, цей стандарт став додатковою гарантією відсутності зловживань у сфері захисту персональних даних. Утім, Конвенція 108+ усе ще залишається надміру загальним і застарілим актом, положення якого значною мірою були уточнені й доповнені іншими регуляторними документами. Одним з них став GDPR.

GDPR. Регламент ЄС, що набув чинності у 2018 році, значно детальніше підходить до стандартів захисту персональних даних. Так, серед принципів з'явилися вимоги щодо згоди суб'єкта на обробку інформації про нього. Зокрема, GDPR уточнює, що згода має

бути вільною та поінформованою, тобто особа має усвідомлювати, які саме дані й для чого збираються, кому їх можуть передати тощо, а також мати право відкликати згоду на обробку даних у разі потреби. Окрім того, документ уточнює й **підстави для обробки чутливих даних,** їх можна узагальнити таким чином:

- передбаченість обробки даних безпосередньо на рівні закону;
- обробка даних на підставі згоди суб'єкта;
- обробка необхідна для захисту життєво важливих інтересів суб'єкта;
- обробку здійснюють неприбуткові організації у зв'язку з метою їхньої законної діяльності;
- обробка даних, які відкрито оприлюднені суб'єктом;
- обробка, необхідна в судовому процесі;
- обробка, необхідна в медичних цілях або для захисту публічного здоров'я;
- обробка здійснюється заради суспільного інтересу, у наукових, статистичних чи історичних цілях.

В інших випадках обробка чутливих даних заборонена. Утім, і серед зазначених підстав є такі, що дозволяють обробку даних про походження, стать чи сексуальну орієнтацію для надання гуманітарної допомоги, як-от згода особи чи захист її життєво важливих інтересів або публічний інтерес (Пояснення 46, 73 і 112 до GDPR прямо передбачають таку можливість). Подібний режим набагато більш безпечний, адже обмежує організації в праві обробляти чутливі дані без належних на те підстав, а також підводить їх до принципу мінімізації даних: якщо можливо надати допомогу, при цьому отримати менше даних, то організації краще послуговуватися цією опцією.

Додатково GDPR встановлює вимоги до національного регулятора у сфері захисту даних — державного органу, який розроблятиме технічні стандарти та здійснюватиме нагляд за дотриманням законодавства іншими державними органами, приватними організаціями та компаніями. Важливо, що обов'язки покладаються і на самі компанії: вони мають створити інституцію / призначити **особу, відповідальну за контроль за дотриманням законодавства про захист персональних даних.**

Також GDPR впроваджує низку нових прав для суб'єктів персональних даних:

- право бути поінформованим;
- право доступу до своїх персональних даних;
- право на виправлення неповної або неточної інформації;
- право на видалення інформації (право на забуття);
- право на заперечення проти обробки даних;
- право на відкликання згоди;
- право на відмову від автоматизованої обробки даних.

Тож GDPR встановлює більш чіткі вимоги, і багато з них прямо застосовні до випадків обробки даних при наданні допомоги. Наприклад, коли йдеться про чутливу інформацію, її зберігання і видалення. Також Регламент розширює права суб'єкта й дозволяє запитувати видалення даних та оновлення інформації, якщо вона застаріла. Важливою є й можливість

вимагати обробки даних живою людиною, а не автоматизованою системою. Це актуально для випадків, коли прикордонники чи надавачі допомоги ідентифікують осіб за допомогою систем розпізнавання обличчя, які мають високий індекс помилок і неточностей. Загалом будь-яка автоматизована обробка даних може призвести до значної шкоди, тож додаткові гарантії — це позитивний крок, особливо для таких сфер, як гуманітарна допомога (де GDPR, безсумнівно, застосовний).

Як щодо більш «гуманітарних» стандартів? Окрім загальних документів, актуальні й галузеві норми — переважно у сфері надання гуманітарної допомоги й захисту персональних даних вони мають характер так званого м'якого права. Тобто ці стандарти швидше рекомендаційні, ніж обов'язкові. Проте, вони видані профільними організаціями, до позиції яких дослухається більшість добросовісних інституцій. Окрім того, вони містять уже згадані загальні стандарти, адаптовані до контексту збройних конфліктів і надзвичайних ситуацій. Тож розглянемо спеціальні норми, застосовні до захисту даних при наданні гуманітарної допомоги.

Основоположним документом є Довідник щодо захисту даних під час гуманітарних акцій, розроблений МКЧХ. Передумовою його напрацювання стала потреба поєднати правові режими права з прав людини та гуманітарного права, які одночасно діють під час збройних конфліктів. Хоча перші кроки вже були зроблені при розробленні Пояснень до GDPR і рекомендацій на рівні ООН, Ради Європи та інших регіональних органів, переважно їм бракувало належної контекстуалізації та оцінювання ризиків, які притаманні роботі з даними під час конфліктів. Тож провідні експерти напрацювали понад 300-сторінковий документ, який окреслює ключові принципи роботи з персональними даними під час гуманітарних акцій (як безпосередньо надання гуманітарної допомоги, так і евакуації, пошуку зниклих осіб, роботи з військовополоненими тощо). Окрім того, перевага Довідника полягає в тому, що його можна застосовувати незалежно від особливостей національного регулювання. Якщо оцінювати його в контексті цього дослідження, то описані нижче стандарти застосовні як до міжнародних організацій, що надають гуманітарну допомогу в Україні, так і до національних правозахисних, благодійних і гуманітарних організацій.

Принципи. Як і будь-який інший документ, що має на меті врегулювати суспільні відносини з правової точки зору, вступна частина Довідника починається з принципів роботи з даними під час гуманітарних акцій. На відміну від GDPR, Довідник не просто перелічує принципи, а й деталізує їх, наводить приклади застосування на практиці. Які принципи згадує Довідник?

- **Принцип законності роботи з персональними даними.**Окрім дотримання вимог міжнародних документів (на кшталт GDPR чи Конвенції 108+) і національних стандартів держави, у якій організації надають гуманітарну допомогу, на думку МКЧХ, цей принцип охоплює ще й прозорість і передбачуваність процесів, які гуманітарні організації мають забезпечити для суб'єктів персональних даних. Так, особа, яка звертається по гуманітарну допомогу, має розуміти, що відбуватиметься з її даними і за яким законодавством здійснюватиметься їх обробка.

- **Принцип обмеження обробки даних конкретною метою.** На відміну від інших більш загальних документів, Довідник прямо зазначає сім цілей, з якими може здійснюватися обробка даних у гуманітарному контексті. Зокрема: безпосередньо надання гуманітарної допомоги; возз'єднання родин, чиї члени були розлучені внаслідок збройного конфлікту; надання захисту особам і будівлям, які мають захищений статус відповідно до права прав людини та гуманітарного права; медична допомога; захист домівок і доступу до води; ідентифікація осіб та інтеграція їх у національні системи (наприклад, за допомогою інституту надання притулку чи статусу біженця). Перелік цілей вичерпний.

- **Принцип пропорційності.** Збір персональних даних у такій кількості, яка вичерпно потрібна для виконання функцій гуманітарної організації. Водночас Довідник пропонує декілька раціональних уточнень, наприклад наводить випадки, коли мета збору даних

досить широка на момент їх збору через надзвичайність ситуації. У таких ситуаціях принцип пропорційності передбачає видалення надмірно зібраних даних, щойно організації стане відомо, що така інформація не потрібна для виконання гуманітарних функцій.

- **Принцип мінімізації даних.** Цей принцип певною мірою похідний від принципу пропорційності, утім, він більш заточений на захист суб'єкта від надмірного збору даних, які загалом можуть бути релевантними для досягнення мети. Так, існує вимога, щоб гуманітарна організація виконувала свої функції, збираючи мінімальну можливу кількість особистої інформації про отримувачів допомоги. Наприклад, часто виникають дискусії щодо легальності збору біометричних даних від біженців (сканування сітківки ока, розпізнавання облич тощо), який здійснюють не прикордонники при в'їзді в країну, а гуманітарні організації при наданні допомоги. Фактично цей принцип червоною ниткою проходить через усі активності й передбачає не лише лімітований збір даних, а й обмеження строків їх зберігання, своєчасне видалення застарілих або непотрібних даних, анонімізацію даних тощо.

- **Принцип підтримання належної якості даних.** Зокрема, організації мають стежити за тим, щоб дані були актуальними й належним чином оновлювалися. Це важливо у випадках надання гуманітарної допомоги протягом певного часу, наприклад року, коли люди можуть змінити прізвище, одружитися чи коли відбуваються інші події, які впливають на отримання підтримки та її розмір.

- **Принцип безпеки й захищеності даних.** Організації, які надають гуманітарну допомогу, гарантують, що персональні дані будуть належним чином захищені технічно в питаннях зберігання й доступу інформації, а також не будуть нелегально передані третім особам, маючи належний рівень правового захисту.

Багато додаткових принципів згадується і в інших документах м'якого права. Наприклад, Міжвідомча постійна комісія в Оперативному керівництві щодо відповідальності за дані в гуманітарній діяльності розділяє принципи обробки персональних даних та інформації, яка збирається під час надання гуманітарної допомоги, але не є персональними даними. Так, для неперсональних даних Комісія виокремлює принцип **відповідальності й підзвітності** (для організацій, які здійснюють обробку даних), **конфіденційності** (для інших департаментів організації, третіх осіб і держави), **безпеки даних, людиноцентризму** в процесах обробки й збору даних, **кооперації між партнерами** щодо надання гуманітарної допомоги (для держави, громадянського суспільства, міжнародних організацій тощо) і кілька похідних принципів (як-от, видалення даних). Утім, варто відзначити, що згадані принципи цілком застосовні й до обробки персональних даних: важко уявити, що робота з інформацією, яка передбачає ідентифікацію осіб, не відповідатиме принципу конфіденційності, безпеки чи відповідального ставлення до даних.

Схожий перелік надав і Офіс ООН з координації гуманітарних питань, який у Керівництві щодо відповідальної роботи з даними наголосив на необхідності орієнтувати процеси роботи з персональними даними в гуманітарному секторі на захист прав людини. Окрім того, він категоризував усі принципи за трьома основними напрямами:

Безпека	Етичність	Ефективність
Юридична та технічна безпека даних на всіх етапах їх обробки	Дотримання принципів етики даних та етики роботи в гуманітарному секторі	Здатність досягнути мети збору даних

На цих трьох основоположних стовпах побудований увесь підхід інституцій ООН до захисту персональних даних. Наприклад, під час роботи над окремою Стратегією роботи з даними під час пандемії COVID-19, наголошувалося на безпеці даних, їх конфіденційності й ефективному менеджменті обігу даних у межах допоміжних інституцій ООН. Аналогічний підхід простежується в Дорожній карті Генерального секретаря ООН, який підкреслив необхідність забезпечити захищеність даних і посилити міжвідомчу співпрацю за цим напрямом.

Як помітно з аналізу основних рекомендаційних документів у цій сфері, міжурядові та неурядові організації перебувають «на одній хвилі» щодо принципів роботи з персональними даними. Фактично вся робота зводиться саме до виховання серед організацій, які виконують гуманітарні функції, відповідального ставлення до роботи з персональними даними. Формування такого ставлення можливе саме завдяки розробленню універсальних принципів. Крізь їх призму й оцінюється правомірність роботи з персональними даними, зокрема формування загальних політик. Утім, розроблення політик та оцінювання ризиків і загроз для прав людини не є фінальною точкою в цій історії. Значно важливіше практичне застосування таких політик до реальних сценаріїв.

Збір даних далеко не завжди передбачає внесення ПІБ і номеру паспорта в паперовий бланк. Сьогодні все частіше використовують цифрові технології: збір даних може мати форму розпізнавання обличчя автоматизованою системою, збору кукіз на вебсайті, де отримувач допомоги має зареєструватися, завантаження документів у спільні бази даних тощо. У таких випадках для організацій, які надають допомогу, важливо пересвідчитися, що вони мають законні підстави для збору даних. Однією з найпоширеніших підстав для обробки особистої інформації є згода особи. Утім, навіть до неї є окремі вимоги етичного та правового характеру.

Згода особи. У Довіднику МКЧХ наведено характеристики згоди на обробку персональних даних, які роблять її валідною. Зокрема, згода особи має бути:

- **Інформована.** Особу мають повідомити про вид персональних даних, які збирають для надання гуманітарної допомоги, мету їх збору (чому саме ці дані необхідні), термін і порядок зберігання персональних даних, підстави для передачі персональних даних третім особам (як-от іншим організаціям чи державі), а також умови виправлення та видалення застарілих і неточних даних. Недостатньо просто сказати, що персональні дані збирають, особа має повністю розуміти всі процеси, у яких її персональні дані будуть задіяні. Лише в такому випадку згода є інформованою.

- **Чітка.** В ідеалі згода має надаватися в письмовій формі на спеціальному бланку, який також містить політику конфіденційності організації, яка надає гуманітарну допомогу. Так, у разі спору можна встановити, чи згода справді була надана. Якщо неможливо отримати згоду в письмовій формі, її можна записати на відео з дозволу особи, яка надає таку згоду. Утім, вона має бути зрозумілою й чітко віддзеркалювати позицію особи.

- **Своєчасна.** Згода має надаватися до отримання гуманітарної допомоги. Порушенням є надання допомоги з відповідною обробкою персональних даних, після якої організація вимагає надати згоду на такі процеси. Зокрема, тому, що особа не зможе заперечити чи запобігти використанню її даних, а також відмовитися від допомоги.

- **Вільна.** Згода вважається вільною, якщо особа може відмовитися від отримання допомоги. Наприклад, особа може вважати обсяг оброблюваних даних надмірним чи не бажати залишати певну інформацію гуманітарній організації. Окрім того, особа має право відмовитися від автоматизованої обробки даних. У такому випадку їй мають запропонувати обробку даних живою людиною. Також особа має усвідомлювати всі наслідки збору і обробки її даних.

- **Така, що враховує вразливе становище особи.** Соціальне, культурне та релігійне

становище особи має враховуватися при зборі персональних даних. Процес збору персональних даних слід здійснювати з повагою до особливостей особи, враховуючи:

- неграмотність, наявність / відсутність інвалідності, вік, стан здоров'я, гендер і сексуальну орієнтацію;
- місцезнаходження особи (як-от тимчасовий притулок, місце обмеження чи позбавлення свободи, віддалене місце з обмеженим зв'язком тощо);
- мову спілкування, незнання юридичних особливостей країни, де вона отримує допомогу тощо (так, іноземні та міжнародні організації мають пересвідчитися, що населення регіону, де вони працюють, розуміє зміст обробки даних);
- приналежність до політичної, етнічності чи соціальної меншості / більшості;
- потенційний вплив технологій на особу, якщо вони мають вади щодо, наприклад, людей кольору, залежно від статі чи інших характеристик (як це часто стається з технологіями розпізнавання облич).

- **З можливістю відкликання.** На будь-якому етапі обробки даних особа має право відкликати згоду та вимагати видалення всієї інформації про неї. При цьому її мають повідомити про наслідки відкликання згоди. До відкликання згоди застосовуються всі правила, як і до згоди: воно не має здійснюватися під тиском третіх осіб, має бути інформованим і своєчасним. У таких випадках багато запитань виникає щодо систем, де згода надається шляхом проставлення «пташки» у відповідному вікні на вебсайті. З одного боку, згода вважається вільною та поінформованою, з іншого — чи можливо відкликати її та вимагати припинити обробку даних, якщо вебсайт чи форма не мають технічної підтримки або зв'язку з живою людиною? Аналогічною є ситуація і з кукібанерами, які збирають інформацію про активність у мережі.

І хоча, окрім згоди, існує ще досить велика кількість підстав правомірної обробки даних, більшість з них залежать скоріше від тлумачення обставин, аніж поведінки суб'єкта даних чи належних дій гуманітарної організації. Наприклад, наявність публічного інтересу чи загрози життєво важливим інтересам особи надто контекстуальний критерій, щоб напрацювати типову практику, застосовну в будь-якому випадку. Водночас саме з формою згоди виникає найбільше запитань. Проте навіть за умови легального збору інформації що робити з даними після їх отримання?

Зберігання персональних даних. Основними вимогами до зберігання персональних даних є насамперед забезпечення їх технічної безпеки — особливий (і обмежений) режим доступу до серверів, безпечне розташування серверів (уникнення держав з високим індексом порушення прав людини чи безпосередньо персональних даних, окупованих територій чи територій з невизначеним правовим режимом), уникнення зберігання даних на серверах компаній, які порушують права людини тощо. Загалом у цьому питанні важлива ще й політика прозорості щодо порядку зберігання даних: щонайменше, особу можна попередити, у якій саме державі розташовані сервери і яке законодавство буде застосовним у разі виникнення суперечливих ситуацій.

Права особи відносно її персональних даних. Окрім процедурних питань, які залежать більшою мірою від діяльності гуманітарних організацій, що збирають дані, Довідник МКЧХ та інші документи передбачають безпосередньо права суб'єктів даних. Серед них ключовими є можливість виправити застарілі дані, змінити дані чи видалити їх на запит особи, а також право заперечувати проти обробки даних (чи певного типу їх обробки). Розглянемо, що на практиці означає кожне з цих прав.

- **Право на виправлення та зміну даних.** Особа, чиї дані обробляються, має право вимагати від організації виправити інформацію в разі, якщо до бази даних було внесено неповну, неточну чи застарілу інформацію про неї. Це можливо зробити і без доказів правильності інформації в разі, якщо дані не важливі (одруківка, технічна помилка тощо). У випадках, коли дані важливі для визначення юридичного статусу особи, виправити їх можна шляхом надання додаткової інформації (документи, що вказують вік, деталі щодо статі, кількості дітей, громадянства тощо). Виправлення даних відбувається

у випадках, коли сталася помилка, тоді як зміна даних — коли дані, надані особою, були правильними, але з плином часу вони змінилися. Наприклад, після одруження змінилося прізвище, сім'я отримала статус багатодітної тощо.

- **Право на видалення даних.** Довідник передбачає декілька підстав для видалення даних: дані більше не потрібні для надання гуманітарної допомоги, відкликано згоду на обробку даних, суб'єкт заперечує проти обробки даних чи обробка більше не відповідає технічним і правовим вимогам щодо захисту персональних даних. Відмову в задоволенні права на видалення інформації суб'єкт може отримати, якщо обробка даних необхідна для захисту інтересів інших осіб, доказу порушень гуманітарного права чи права прав людини, є підставою правових позовів тощо, словом, за наявності легітимного інтересу в подальшій обробці такої інформації. Підстави, утім, можуть змінюватися залежно від законодавства країни, у якій гуманітарна організація надає допомогу чи зареєстрована.

- **Право на заперечення проти обробки даних.** Заперечення проти обробки даних є менш радикальною формою відмови порівняно з вимогою видалення даних. Воно, зокрема, передбачає можливість продовжити зберігання інформації організацією без здійснення інших видів обробки даних, як-от аналізу для статистики, передачі даних тощо. Утім, як і в ситуації з видаленням даних, у цьому випадку можливе продовження обробки даних гуманітарною організацією за наявності легітимних підстав.

Видалення даних за строком давності. Загалом згадані вище принципи мінімізації даних і пропорційності прямо вказують на те, що використання та зберігання даних довше, ніж це необхідно для виконання мети їх збору, буде порушувати права людини. Тому основним завданням організації є встановити той момент, коли інформація припиняє бути необхідною. Довідник МКЧХ, зокрема, містить для цього трискладовий тест:

- оцінювання природи й чутливості даних;
- оцінювання формату зберігання даних;
- оцінювання кількості даних і типу їх носіїв.

Відповіді на ці питання дозволять з'ясувати, яким чином і в які строки слід знищувати дані. У деяких випадках дані можна анонімізувати чи псевдонімізувати й потім використовувати в статистичних чи прогностичних цілях. Наприклад, заміщення ПІБ конкретними символами чи іншими позначками до такої міри, що дані більше неможливо зіставити з конкретною особою. Хоча гуманітарні організації мають зважувати, чи пропорційно це до витрат на такі заходи, якщо інформація зберігається на паперових носіях, то навряд повна анонімізація буде можливою, а цифровізація даних потребуватиме додаткової згоди особи (якщо її одразу не отримали на таку обробку даних). Після видалення чи іншого знищення даних уповноважена особа має пересвідчитися, що дані неможливо відновити та що вони не були переміщені на інші сторонні носії.

Передача даних третім особам. Проблемним питання захисту даних стає тоді, коли відбувається передача даних третім особам — державі, іншим організаціям, субпідрядникам для виконання певних завдань тощо. Причин для цього може бути безліч: наприклад, організація може уточнювати дані в місцевих партнерів чи обмінюватися з ними інформацією, щоб належним чином спланувати гуманітарні акції, надавати дані підрядникам для виготовлення засобів для осіб з особливими потребами, передавати дані при звітуванні донорським організаціям. Коли відбувається будь-який процес передачі даних, важливо пам'ятати про декілька простих правил:

- організації й особи, яким передають персональні дані, мають забезпечити аналогічний рівень технічного та правового захисту, як і ті, які збирали дані та отримували згоду особи на їх обробку та передачу;

- використання даних третіми особами з метою, яка не відповідає меті збору даних, порушує правила роботи з персональними даними;

- осіб, чиї дані заплановано передавати третім особам, потрібно попереджати про таку передачу інформації та її мету. Наприклад, Офіс ООН з координації гуманітарних питань тривалий час мав проблему, що біженцям не пояснювали належним чином процеси, які відбуваються з їхніми персональними даними, у тому числі і передачу інформації третім особам (свідчення біженців з Лівану навіть стали публічними при ретроспективному оцінюванні цього питання);

- передача даних донорським організаціям має відбуватися в анонімізованому або псевдонімізованому вигляді, враховувати потенційні ризики повторної ідентифікації, витоків даних, надійності донорського захисту даних, реальних потреб в отриманні такої інформації та використання її відповідно до мети отримання даних (що передбачає також дотримання принципів прозорості та відповідального ставлення до даних самими донорськими організаціями). Організації, які збирають персональні дані, також мають попереджати, що чутлива інформація може передаватися донорським організаціям для звітування;

- співвіднесення обмежень на поширення даних з принципом інтероперабельності систем (якщо системи взаємодіють, кожна з них потребує менше даних для того, щоб повноцінно функціонувати, наприклад для ідентифікації особи). Так, система «Eurodac» у ЄС не взаємодіє з базою даних ООН в Офісі з координації гуманітарних питань, що створює певні незручності, адже на обох рівнях доводиться збирати дані з нуля. З іншого боку, такий суворий режим доступу й передачі даних убезпечує інформацію від потрапляння до урядів, адже дуже часто персональні дані використовують для трекінгу осіб через різні додатки, відстеження їх місця перебування, роду занять тощо.

- при передачі даних транскордонно слід зважати на рівень захисту прав людини в державі, де оперують треті особи, які отримують дані. Наприклад, не варто передавати дані в авторитарні режими, де дані можуть отримати поліція чи безпекові служби й згодом використовувати для переслідування вразливих осіб. Оцінювання має проводитися в кожному випадку, але часто організації послуговуються чинними рейтингами та індексами захисту прав людини, розробленими міжнародними організаціями (наприклад, індекс свобод від Freedom House).

Оцінювання впливу на права людини. Важливо, що багато міжнародних документів орієнтовані саме на створення рамкових тестів, щоб організації, які надають гуманітарну допомогу, могли самостійно пересвідчитися, чи вони належно працюють з персональними даними або даними, які сукупно можуть призвести до ідентифікації особи. Наприклад, уже згадані Оперативні керівництва щодо відповідальності за дані в гуманітарній діяльності від Міжвідомчої постійної комісії прямо наголошують на необхідності оцінювання впливу операцій з обробки даних на безпеку даних і права людини. Причому таке оцінювання має декілька рівнів: воно має проводитися як усередині організацій, так і відносно зовнішніх загроз. Рамковими документами щодо порядку проведення оцінювання впливу на права людини є Довідник МКЧХ і Керівництва від французького регулятора з питань захисту персональних даних.

- **Внутрішній контроль.** Вимога внутрішнього контролю відповідає стандартам GDPR щодо регулярного перегляду політик роботи з даними та оцінювання ризиків при ухваленні критичних рішень. Це стосується як оцінювання стратегічних планів роботи з даними, так і аналізу тактичних рішень. Наприклад, якщо існує ризик, що територія, де надавалася гуманітарна допомога, опиниться під окупацією, чи доцільно продовжувати зберігати дані, чи варто знищити інформацію, яка міститься на носіях у зоні ризику тощо. У внутрішньому оцінюванні важливу роль відіграють так звані уповноважені із захисту даних, які мають бути в кожній організації та відповідати за дотримання і впровадження на практиці стандартів GDPR та інших регуляцій, оцінювання ризиків та оновлення політик. У контексті збройних конфліктів така особа має бути обізнана у вимогах міжнародного гуманітарного права.

- **Зовнішні аудити.** Залежно від предмета оцінювання, гуманітарні організації також

можуть залучати й зовнішніх аудиторів за умови дотримання ними принципів конфіденційності й безпеки. Це може включати і організації громадянського суспільства, і професійних аудиторів з безпекових питань. Такий аудит має відбуватися відповідно до стандартів, які частково викладені в згаданих Довіднику та Керівництвах.

Вимога проведення оцінювання ризиків, зрештою, підштовхує до створення внутрішніх правил роботи з персональними даними. Чому це актуально? Розглянемо декілька відносно нових ризиків для гуманітарних організацій. Так, актуальну дорожню мапу ризиків розробила правозахисна організація Privacy International.

Телекомунікації. Завжди існує ризик перехоплення повідомлень, які можуть містити чутливі дані, використання інформації для дискредитації гуманітарної організації, переслідування цивільних осіб тощо. Також це може ставити під загрозу й працівників організацій, адже таким чином можна відстежувати їх пересування та адресатів гуманітарної допомоги. І хоча ці ризики частково можливо подолати за допомогою використання захищених сервісів комунікації, багато організацій та їхніх працівників усе ще нехтують можливістю витоку даних та стеження.

Месенджери та соцмережі. Проблема надмірного покладання на соцмережі та месенджери полягає в тому, що вони часто використовують забагато персональних даних, мають доступ до інших функцій девайсів, як-от камери телефону чи сховища даних ноутбука. Окрім того, частота та час використання сервісів дозволяє зрозуміти приблизне місце перебування особи, розпорядок дня, відстежити контакти та пересування за допомогою геолокації тощо. Із соцмережами існує ще більша проблема: гуманітарні організації не мають жодного впливу на їхню бізнес-модель, передачу даних третім особам, захищеність від витоку даних. Ба більше, використання сервісів платформ може сприяти додатковому моніторингу їхньої активності державою чи нелегальними організаціями (терористами, екстремістами).

Смарткартки. Це пристрої, схожі на електронні гаманці, відстежування яких дозволяє з'ясувати місце перебування та рух особи, кількість витрат і часові рамки діяльності особи. Часто гуманітарні організації не можуть напряму надавати допомогу, а тому послуговуються онлайн-транзакціями, що може створити додаткові ризики для приватності осіб.

Технології стеження. Гуманітарний сектор та організації громадянського суспільства часто бувають об'єктом стеження з боку держави та нелегальних організацій. Якщо гуманітарні організації надають допомогу вразливим верствам населення, їм слід бути надзвичайно обережними в тому, що різноманітні трекінгові додатки та шкідливе програмне забезпечення може потрапити до робочих девайсів, баз даних і технологій. Окрім того, використання сервісів небезпечних провайдерів, незахищених комунікаційних мереж і програмного забезпечення, яке не пройшло перевірку на відповідність стандартам у сфері прав людини і захисту персональних даних, може створити додаткові ризики витоку інформації.

Технічні несправності. Важливу роль у захисті та якості зібраних даних також відіграють технології, які гуманітарні організації (або ті, з ким вони співпрацюють для отримання даних) використовують для збору інформації та її обробки. Наприклад, під час застосування технологій розпізнавання облич або відбитків пальців важливо, щоб вони правильно ідентифікували особу, а також були інтероперабельними. Дискусія щодо цього тривала в контексті системи «Eurodac», яка застосовується в ЄС. Так, якщо існує декілька систем, які ідентифікують особу, за умови інтероперабельності кожна з них збиратиме значно менше даних. Якщо ж вони не будуть пов'язані одна з одною, кожна із систем потребуватиме значно більше інформації для кожного випадку ідентифікації.

Кібероперації та кібератаки. Багато гуманітарних організацій мають недостатній рівень експертизи й технічного захисту для того, щоб вчасно виявити й належним чином відповідати на кібератаки проти них. Це часто призводить до витоків даних або знищення баз даних, як уже сталося з базами даних Save the Children, Human Rights Watch та інших

правозахисників у 2020 році. Кібероперації сторін збройного конфлікту можуть призводити і до пошкодження інфраструктури організацій, перешкоджаючи їм здійснювати гуманітарну функцію. Саме тому виникає потреба адаптувати технічні стандарти до контекстів війни й розробити кризові протоколи, які можна буде застосовувати в надзвичайних випадках.

Держави, що порушують права людини. Це особливо актуально в контексті встановлення окупаційних режимів авторитарними державами. Наприклад, в Україні на окупованих територіях діють російські провайдери, російські системи стеження, правовий режим, який дозволяє правоохоронцям мати необмежений доступ до серверів приватних компаній та організацій тощо. Окрім того, є свідчення, що російська поліція та адміністрації збирають персональні дані українців для нібито роздачі гуманітарної допомоги чи здійснення перепису населення, хоча по факту згодом використовують отриману інформацію для переслідування журналістів, членів сімей військовослужбовців, правозахисників й активістів. Навіть у випадках, коли йдеться про демократичні держави, наприклад членів ЄС, виникає питання: чи пропорційний доступ органів правопорядку до більшості баз даних, як-от інформації про мігрантів, шукачів притулку, отримувачів допомоги тощо. Часто поліція та служби безпеки мають доступ до більшої кількості даних, ніж об'єктивно потрібно для їхньої роботи.

Як висновок, існує досить розгалужена система стандартів захисту даних організаціями, які надають гуманітарну допомогу. Утім, проблема полягає скоріше в статусі таких стандартів як актів м'якого права, та відсутності механізму покарання за порушення, особливо з огляду на те, що багато організацій діє транскордонно. Водночас регіональні нормативні регулівні акти часто не здатні адекватно врахувати реалії збройних конфліктів, тоді як поява нових технологій і нових викликів лише ускладнює завдання гуманітарних організацій із захисту персональних даних. Проте загальний характер вимог міжнародного права можна адаптувати на національному рівні, задавши необхідний контекст і знявши деякі ризики шляхом видання роз'яснень національними регуляторами. Тож у контексті збройної агресії Росії в Україні слід розглянути українське законодавство для того, щоб повноцінно оцінити ландшафт і безпеку для діяльності гуманітарних організацій у питаннях захисту персональних даних.

РОЗДІЛ ІІІ.
Композиції захисту даних по-українськи

Відповідно до статистики ООН, лише 71 % країн має законодавство, що передбачає захист персональних даних, тоді як в інших державах регулювання або перебуває на стадії законопроєктів, або взагалі відсутнє. Гуманітарні організації, що працюють або зареєстровані В Україні, окрім міжнародних, радше рамкових стандартів, мають керуватися національним регулюванням. У сфері надання гуманітарної допомоги спеціальним актом, безперечно, буде Закон України «Про гуманітарну допомогу», який визначає і вимоги до оформлення допомоги, і умови її надання. Утім, перш ніж дискутувати щодо таких вимог, слід з'ясувати, як українське законодавство розуміє гуманітарну допомогу (зокрема, під час збройного конфлікту).

Закон дозволяє надання гуманітарної допомоги як громадським і благодійним організаціям, внесеним до Єдиного реєстру отримувачів гуманітарної допомоги, так і безпосередньо фізичним особам. Водночас цей Закон жодним чином не регулює питання захисту даних набувачів допомоги, навіть не робить відсилки до профільного Закону України «Про захист персональних даних». З одного боку, це вказує на те, що законодавець не надто замислювався над захистом даних у надзвичайних ситуаціях, не розробивши спеціальних правил. З іншого — це означає, що загальні правила законодавства про захист персональних даних застосовні в таких обставинах.

> **Гуманітарна допомога** — це цільова безоплатна допомога в грошовій або пожертвувань, виконання робіт чи надання послуг від іноземних чи вітчизняних донорів отримувачам допомоги в Україні чи за кордоном, які потребують її через соціальну незахищеність, незабезпеченість, важке фінансове становище, виникнення надзвичайного стану чи тяжку хворобу, а також для підготовки до збройного захисту держави та її захисту у разі збройного конфлікту.

То що ж передбачає Закон України «Про захист персональних даних» і чи містить він спеціальні норми, чинні на час надзвичайного чи воєнного стану? Об'єктом регулювання цього закону є самі **персональні дані** — відомості або сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Ідентифікація відповідно до Закону України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус» передбачає можливість чітко виокремити особу з-поміж інших за допомогою будь-якої інформації, як-от документів, біометричних даних або подібних параметрів.

Дані, які збирають організації для надання гуманітарної допомоги, переважно і мають на меті ідентифікацію особи, щоб уникнути повторного надання одноразової грошової допомоги, надання допомоги для дітей родинам, які їх не мають тощо. І хоча від типу допомоги залежить обсяг і вид зібраної інформації (так, ПІБ, номер паспорта чи телефон збирають практично завжди), до її обробки завжди буде застосовним законодавство про захист персональних даних. Як наслідок, обробка персональних даних можлива лише за умови, якщо наявна одна з підстав, передбачених статтею 11 Закону.

Релевантні **підстави для обробки** (збору, зберігання, передачі тощо) персональних даних у контексті роботи гуманітарних організацій при наданні ними допомоги:

- згода суб'єкта персональних даних на обробку його персональних даних;
- укладення та виконання правочину, стороною якого є суб'єкт персональних даних або який укладено на його користь;
- захист життєво важливих інтересів суб'єкта персональних даних.

Згода суб'єкта. Однією з найпоширеніших підстав обробки персональних даних з метою надання гуманітарної допомоги є отримання згоди особи. Це пояснюється тим, що допомога переважно надається недержавними організаціями, а тому обробка персональних даних на підставі закону не може слугувати належною підставою в такому випадку. Понад те, порівняно з іншими підставами згоду суб'єкта простіше зафіксувати й оформити.

> Відповідно до статті 2 Закону, **згода** — це добровільне волевиявлення особи (за умови її поінформованості) щодо надання дозволу на обробку її персональних даних відповідно до сформульованої мети їх обробки, висловлене у формі, що дає змогу зробити висновок про надання згоди. В Інтернеті згода під час реєстрації в інформаційно-комунікаційній системі (на вебсайті) може надаватися шляхом проставлення відмітки про дозвіл на обробку персональних даних (якщо система не обробляє даних до проставлення такої відмітки).

Отже, Закон встановлює декілька вимог до згоди: вона має бути **добровільною, чіткою, поінформованою й одержаною до початку обробки даних** (за винятком випадків на кшталт захисту життєво важливих інтересів особи чи інших ситуацій, прямо передбачених статтею 11 закону). Такі вимоги до форми й характеру згоди формально відповідають міжнародним стандартам захисту персональних даних під час збройних конфліктів і надання гуманітарної допомоги. Проте на практиці проблеми виникають з адекватним інформуванням отримувачів допомоги про те, скільки даних збирають, кому їх можуть передавати (наприклад, не зазначено, що донорські організації матимуть доступ до бази даних), а також формою повідомлення — занадто юридичні формулювання того, куди і як передається інформація призводить до нерозуміння наслідків згоди.

Зрештою, серйозною проблемою наразі є фактична неможливість відмовитися від надання персональних даних у таких обставинах — в умовах збройного конфлікту люди перебувають у безвихідному становищі й часто не мають альтернативних джерел доходів, засобів до існування чи способів задовольнити побутові потреби. Як наслідок, надання згоди є лише формальністю, тоді як на практиці можливості відмовитися в осіб немає. Це також слід враховувати для запобігання зловживанням з боку гуманітарних організацій. Як варіант, у випадках, коли особа не хоче, щоб її персональні дані зберігалися в гуманітарній організації, замість відомості видачі гуманітарної допомоги, де зазначені її персональні дані, відповідальна посадова особа може складати звіт про отриману й розподілену гуманітарну допомогу, він буде належною підставою для списання гуманітарної допомоги з балансу організації.

Чи обов'язково згода має бути письмовою? Закон України «Про захист персональних даних» не обмежує форми для висловлення згоди на обробку персональних даних. Утім, організація, яка надає гуманітарну допомогу, у разі виникнення спору муситиме довести, що згода на збір та обробку даних таки була надана. Тому для уникнення непотрібних суперечок варто фіксувати факт надання згоди. Наприклад, деякі організації послуговуються фотофіксацією як для звітування про належний розподіл допомоги, так і убезпечення себе від можливих судових позовів про незаконний збір даних. У цьому випадку важливо пам'ятати, що слід запитати згоду особи на запис, адже вважається, що сам факт позування (коли особа дивиться на об'єктив фотоапарата) є формою згоди.

Водночас правозахисники зазначають, що у випадках, коли людина телефонує в тимчасові пункти допомоги чи колцентри, питання про прізвище та ім'я, номер телефону чи адресу електронної пошти не є надмірними, адже мають на меті не збір інформації, а перевірку особи. Тому в таких ситуаціях фіксувати згоду особи на обробку даних не потрібно. Водночас, якщо телефоном збираються дані для надання певної послуги, а потім така інформація буде зберігатися чи додатково опрацьовуватися, згода буде потрібною.

Факт згоди на фото для звітування донорським організаціям і для підтвердження особи в цілях отримання гуманітарної допомоги **не означає згоду на поширення** таких зображень третім особам або розміщення фото / відео в публічному просторі (наприклад, у соціальних мережах для висвітлення роботи гуманітарної організації). Для таких публікацій організація має отримати окрему згоду особи (стаття 308 Цивільного кодексу України).

Водночас правозахисники зазначають, що у випадках, коли людина телефонує в тимчасові пункти допомоги чи колцентри, питання про прізвище та ім'я, номер телефону чи адресу електронної пошти не є надмірними, адже мають на меті не збір інформації, а перевірку особи. Тому в таких ситуаціях фіксувати згоду особи на обробку даних не потрібно. Водночас, якщо телефоном збираються дані для надання певної послуги, а потім така інформація буде зберігатися чи додатково опрацьовуватися, згода буде потрібною.

Укладання та виконання правочину. Як пояснюють експерти Платформи прав людини, посилаючись на норми Цивільного кодексу України, при укладенні будь-якого договору особа зобов'язана себе ідентифікувати. Так, стаття 28 вказує, що особа набуває прав і обов'язків та здійснює їх під своїм ім'ям, а статті 202 та 626 відповідно вказують, що правочин передбачає набуття, зміну чи припинення прав і обов'язків, у тому числі шляхом укладення договору. Оскільки укладення договору про надання благодійної допомоги саме собою передбачає згоду особи на умови договору, додаткової згоди відповідно до статті 11 Закону України «Про захист персональних даних» уже не потрібно. Водночас частина 2 статті 12 цього Закону передбачає повідомлення особи про те, які саме дані збираються та для яких цілей це здійснюється. Тому в договорі має бути чітко вказано обсяг інформації, яка збирається, і мету її обробки. Якщо цього не зробити, особа матиме право оскаржувати, наприклад, те, що організація збирає надмірну кількість даних чи використовує вже зібрану інформацію не за призначенням (наприклад, у маркетингових цілях тощо).

Захист життєво важливих інтересів особи. Найчастіше ця підстава використовується, коли необхідно надати особі невідкладну медичну допомогу, врятувати її від протиправних посягань чи здійснити аварійно-рятувальні операції. Утім, у випадку гуманітарної катастрофи в певному регіоні можна припустити, що обробку даних гуманітарні організації можуть здійснюватися до отримання згоди особи. Наприклад, нема фізичної можливості чи достатньої кількості часу для роз'яснень, що нівелює правомірність згоди (адже вона має ґрунтуватися на попередньому повному інформуванні), особа перебуває в поганому психоемоційному стані, що унеможливлює роз'яснення тощо. Омбудсмен у своїх роз'ясненнях також зазначає, що ця підстава застосовна у випадках, коли особа в цілому перебуває без свідомості. Утім, основним правилом цієї підстави для обробки персональних даних є отримання згоди особи на обробку даних, щойно це стає можливо.

Якщо після появи можливості згоду особи не було одержано або особа прямо заперечує проти обробки персональних даних, організація зобов'язана **припинити таку обробку та видалити вже отриману інформацію**.

У випадку припинення обробки даних через неотримання згоди, звісно ж, актуальним є питання звітування організацій, які надають гуманітарну допомогу, міжнародним донорам і державним органам, якщо вони співпрацюють. Утім, у такому разі гуманітарна організація може вказати знеособлені дані про особу: вулицю проживання без конкретної адреси (у випадках, коли ключовим є походження особи), стать, соціальний статус (особа з інвалідністю, робоча спеціальність тощо), віковий діапазон тощо.

Окрім того, експерти зазначають, що використання персональних даних може передбачати різні дії з їх збору, поширення чи зберігання, утім ключовим залишається відповідність таких дій меті обробки даних. Очевидний приклад: якщо дані збирають винятково з метою

надання гуманітарної допомоги, їх використання у маркетингових цілях буде суперечити вимогам закону. Де можливо, наголошують правозахисники, інформацію про особу можна брати з офіційних документів, виданих на ім'я особи, і публічних реєстрів. Утім, обробка інформації з відкритих джерел усе ще передбачає обов'язок повідомити особу, що її персональні дані використовують для надання тих чи інших послуг, як-от гуманітарної допомоги.

> **Важливо!** При зборі персональних даних для надання гуманітарної допомоги організації мають дотримуватися принципу мінімізації даних. Так, не варто збирати непропорційно великі обсяги особистої інформації, часто непотрібною є інформація про сексуальну орієнтацію, стать чи етнічне походження. Зайвими можуть бути й дані про вік чи сімейний стан, якщо це не важливо для отримання конкретного виду допомоги.

Зберігання персональних даних отримувачів допомоги. Окрім наявності підстав для обробки даних, володілець даних (тобто гуманітарна організація) зобов'язаний створити базу даних осіб, що отримують гуманітарну допомогу, розробити внутрішні правила обробки даних, положення про таку базу (яке буде доступним для отримувачів допомоги, правозахисників, журналістів тощо) і призначити особу, відповідальну за процеси обробки даних і їх захисту. Це зумовлене тим, що розпорядники і володільці даних краще усвідомлюють, які дані і як саме слід обробляти, а також свої технічні спроможності щодо забезпечення захисту серверів, їх розташування та передачі даних між базами даних у випадку, якщо у володільця чи розпорядника їх кілька. Деякі особливості регулювання передбачені Типовим порядком обробки персональних даних, затвердженим наказом Уповноваженого Верховної Ради України з прав людини № 1/02-14 ще у 2014 році. Цей Типовий порядок визначає, поміж іншого, і певні організаційні обов'язки володільців і розпорядників:

- визначення порядку доступу працівників організації до персональних даних;
- визначення порядку обліку операцій, що включають обробку персональних даних;
- розробку плану дій на випадок несанкціонованого доступу до сховища даних, пошкодження технічних систем чи виникнення інших надзвичайних ситуацій (у контексті збройного конфлікту актуальною є можливість окупації території тощо);
- проведення тренінгів із захисту персональних даних для співробітників.

Відповідно до Типового порядку персональні дані потрібно обробляти й зберігати так, щоб унеможливити до них доступ третіх осіб, що особливо актуально, коли йдеться про автоматизовану обробку даних, до якої можливо отримати доступ через мережу Інтернет. З огляду на те, що автоматизовані системи можуть мати технічні несправності, слід зважати й на потребу регулярних технічних оглядів таких систем.

Поширення персональних даних отримувачів допомоги. Як уже згадувалося вище, часто персональні дані, зібрані в процесі надання гуманітарної допомоги, організації мають використовувати для звітування міжнародним донорським організаціям, державним органам тощо. Також дані можуть зберігатися на закордонних серверах, де їхню технічну безпеку забезпечують треті компанії. Особиста інформація може використовуватися із метою побудови логістики та передбачення майбутніх потреб, що часом роблять організації, відмінні від тих, які безпосередньо надають гуманітарну допомогу. Утім, слід пам'ятати, що про будь-який факт поширення персональних даних третім особам гуманітарні організації мають повідомляти заздалегідь, отримуючи на це згоду суб'єкта персональних даних. Понад те, така передача даних має відповідати меті збору даних: наприклад, отримання згоди на передачу даних іншим організаціям для надання гуманітарної допомоги, тоді як фактично організація передаватиме дані для маркетингових цілей чи проведення

досліджень, буде порушенням права на захист персональних даних.

> Третя особа, якій планується передавати персональні дані, має забезпечити дотримання всіх стандартів захисту таких даних як у технічному, так і в юридичному аспекті. Обов'язок перевірити, чи третя особа здатна дотримуватися стандартів, **покладається на володільця даних**, що планує передавати дані, тобто в цьому випадку на гуманітарну організацію.

Годі й казати, що неспроможність забезпечити технічний чи юридичний захист персональних даних передбачає, що дані не можуть бути поширені такій особі, компанії чи організації. Загалом до третіх осіб також застосовне правило про розробку внутрішніх положень, які, зокрема, регулюватимуть доступ працівників до баз даних і серверів, визначатимуть умови видалення чи виправлення даних тощо. При цьому захист потрібно забезпечувати не лише організації чи особі, яким передані дані, а і в процесі трансферу інформації. Постає актуальне питання: а що робити, коли гуманітарна організація діє на окупованій території чи території, прилеглій до окупованої, у так званій сірій зоні?

Як обробляти персональні дані під час воєнного стану? Попри поширені очікування, тенденції з боку держави свідчать не про збільшення кількості обмежень, а радше посилення захисту персональних даних. Оскільки, для війни в Україні характерні динамічність лінії фронту й зміна статусу територій (окуповані, деокуповані, прифронтові та прикордонні зони), важливим питанням є захищене зберігання даних. З 12 березня 2022 року чинною є постанова Кабінету Міністрів України «Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану», якою заборонено використання хмарних ресурсів і центрів обробки даних, розташованих на тимчасово окупованих територіях України. Експерти загалом підтримують таке обмеження, адже це дозволяє уникнути ситуацій захоплення баз даних і використання їх окупантами для переслідування журналістів, активістів, правозахисників та інших вразливих груп населення, які беруть участь у наданні гуманітарної допомоги або отримують її. Так само заборона поширюється і на хмарні ресурси і сховища, які розташовані на території держави-агресора, належать суб'єктам, зареєстрованим у ній (наприклад, сховище даних у Німеччині, засноване російською компанією) або державах, що входять до митних чи воєнних союзів з державою-агресором. Таким чином, обмеження стосуються не тільки Росії, а і Білорусі та країн низки інших пострадянських країн.

Ініціативи, які непрямо впливають на захист персональних даних в гуманітарній сфері. Це переважно стосується доступу державних органів до баз даних, у тому числі тих, володільцями чи розпорядниками яких є приватні організації (українські та іноземні). Серед найвпливовіших ініціатив варто виокремити зміни до Кримінального процесуального кодексу України:

- **Закон № 2111** від 3 березня 2022 року, який стосується спрощення проведення слідчих дій під час воєнного стану;
- **Закон № 2137** від 15 березня 2022 року, який охоплює зміни процедур огляду місця події, обшуку, тимчасового доступу до комп'ютерних систем і даних, можливість копіювання записів з пристроїв спостереження, що стосується і справ про підозру гуманітарних організацій у шахрайстві (де внаслідок відкриття провадження слідчі матимуть необмежений доступ до баз даних вразливих груп).

На додаток до спрощення самих слідчих процедур, «полегшено» й процес погодження слідчих дій: якщо раніше було потрібно отримати ухвалу слідчого судді, то зараз достатньо звернутися до керівника органу прокуратури у випадках, коли слідчий суддя об'єктивно не може надати такий дозвіл. Тобто щонайменше в цьому випадку при отриманні дозволу треба провести контекстуальне оцінювання обставин, у яких відбувається розслідування.

Ситуація змінилася в липні 2022 року, коли було внесено зміни до статті 615 Кримінального процесуального кодексу України, які стосувалися саме питання доступу до персональних даних. Відповідно до нових правил, введених на час дій воєнного стану, прокурор може санкціонувати тимчасовий доступ до інформації, яка зберігається в особи або в базі персональних даних володільця даних. Як зазначають юристи, на відміну від інших слідчих процедур, ці зміни не залежать від доступності слідчого судді й просто уможливлюють доступ до інформації на приватних серверах лише на підставі рішення прокурора (тільки потім це рішення погоджується з керівником органу прокуратури). Тобто існує ризик непропорційного втручання в хмарні сховища і бази даних, володільцями яких є гуманітарні організації.

Як наслідок, загрози для персональних даних загалом існують у різних площинах: починаючи із зовнішніх загроз у формі хакерських атак, зливів даних і використання баз даних з метою переслідувань вразливих груп і завершуючи потенційним надмірним втручанням держави в такі бази даних, створені гуманітарними організаціями. Оскільки наразі відсутнє спеціальне регулювання обробки персональних даних безпосередньо під час збройного конфлікту і в контексті надання гуманітарної допомоги, організації керуються загальними стандартами захисту даних.

І хоча вже було декілька спроб оновити законодавство у сфері захисту персональних даних й узгодити його з європейськими стандартами та GDPR, один законопроєкт відхилив парламент, тоді як інший досі перебуває на розгляді в профільному комітеті. Це означає, що збір, зберігання й поширення персональних даних наразі має відповідати підставам обробки даних, а також принципам, описаним у двох попередніх розділах, — міжнародним стандартам і чинному національному регулюванню. Чи застосовуються ці стандарти на практиці в роботі українських та іноземних гуманітарних організацій? Це можна з'ясувати, проаналізувавши їхні політики захисту даних і медійний ландшафт на предмет ситуацій порушення правил обробки персональних даних.

РОЗДІЛ IV.
Чи потрапляють гуманітарні організації в такт зі стандартами?

Стандарти захисту персональних даних — як національні, так і міжнародні — мають більш-менш загальний характер. Це логічно, адже вони орієнтовані на величезну кількість організацій різного розміру й порядку роботи, які застосовують різні засоби для обробки інформації та працюють у різних контекстах. Як наслідок, ключовим питанням є не лише те, чи впроваджені стандарти в корпоративні політики компаній, а і те, наскільки якісно вони інкорпоровані і чи можливе їх ефективне застосування на практиці. Тому метою дослідження було встановити, чим керуються компанії при зборі й обробці даних, і з'ясувати, чи відповідають такі політики стандартам і чи можливо покращити практики роботи з персональними даними.

Для зручності аналізу виокремлено чотири основні категорії організацій, які виконують гуманітарні функції. Розподіл за категоріями залежав від особливостей правового регулювання їхньої діяльності (зокрема, питання юрисдикції), порядку формування й адміністрування, способу надання гуманітарної допомоги, а також масштабів роботи організацій. Так, дослідження оцінює політики й практики міжурядових організацій, міжнародних, іноземних і національних гуманітарних організацій.

Міжурядові організації

Ця категорія охоплює тих надавачів гуманітарної допомоги, яких у медіа найчастіше називають просто міжнародними організаціями, — різноманітні органи в структурі ООН (ЮНЕСКО, ЮНІСЕФ, УВКБ ООН тощо), Генеральний директорат Європейської комісії з питань цивільного захисту та гуманітарної допомоги тощо. Усі ці організації мають особливий порядок формування, затвердження програм гуманітарної допомоги та особливі правила роботи з персональними даними. Залежно від виду допомоги різниться обсяг зібраних даних, порядок їх зберігання і обробки, а також спосіб їх збору.

Водночас статус і офіційний статус не захищають від проблем, пов'язаних з витоком даних або кібератаками. Наприклад, у 2019 році відбулася атака на базу даних ООН у центральному офісі у Женеві, що призвело не лише до витоку інформації, а й підриву довіри до інституційної спроможності такої організації, як ООН, захищати дані. Тобто ризики існують не лише для самих персональних даних, а й репутації ключових інституцій і їх здатності надалі забезпечувати надання гуманітарної допомоги. Тож з'ясуємо, чи ключові міжнародні актори мають продумані політики та чи застосовують їх на практиці.

Агентство ООН з питань біженців (далі — УВКБ ООН). Ця інституція стала першою серед структур ООН, яка розробила й успішно впровадила окремі політики щодо захисту персональних даних. Цікаво, що це сталося аж у 2015 році. До того організація, як і всі інші частини ООН, керувалася загальними міжнародними стандартами та національними вимогами. Наразі ж існує окремий документ — Політика щодо захисту персональних даних осіб, важливих для Агентства.

У 2018 році Александр Бек, старший офіцер із захисту даних в УВКБ ООН, наголосив, що розроблення окремої політики щодо захисту мотивована тим, що ключові міжнародні документи не здатні належно адресувати нові загрози для даних, породжені розробленням технологій автоматизованої обробки даних, новими кіберзагрозами, соцмережами тощо. Тож як виглядає сама політика? Розглянемо основні її положення і з'ясуємо, чи вони належно адресують ризики у сфері захисту персональних даних.

Політика щодо захисту персональних даних досить деталізовано пояснює підходи УВКБ ООН до захисту даних та їх передачі третім особам:

- **принципи захисту даних** (наявність легітимної підстави та уточнення мети обробки даних, точність даних, дотримання принципів необхідності та пропорційності, конфіденційність і безпека даних, повага до прав інших осіб та відповідальність за порушення);
- **права суб'єкта персональних даних** (доступ до інформації; виправлення і видалення даних, заперечення проти обробки даних, обмеження, які уможливлюють обробку даних суб'єкта навіть за наявності заперечень з його боку);
- **умови обробки даних** (конфіденційність та безпека даних; технічні вимоги до паролів, доступу до даних, порядку передачі даних усередині організації; повідомлення про порушення порядку захисту даних);
- **вимоги дотримання політики партнерськими організаціями** (у тому числі розірвання партнерських відносин у разі порушення правил захисту даних);
- **передача даних третім особам** (пріоритет збереження довіри до УВКБ ООН та ефективного надання гуманітарної допомоги, особливі правила щодо договорів про передачу даних третім особам, особливі правила передачі даних органам правопорядку, захист даних осіб з імунітетами);
- **наявність відповідальної за захист даних особи** (моніторинг дотримання політики, надання консультацій щодо запровадження нових практик роботи з персональними даними, зберігання документації щодо збору та обробки даних, звітування щодо ефективності політик захисту даних).

Хоча загалом майже 50-сторінковий документ деталізує правила роботи з персональними даними досить суттєво порівняно із загальними міжнародними регуляціями, усе ще залишається актуальним питання того, які саме технології застосовуються. Так, політика не встановлює жодних обмежень на роботу із системами, керованими штучним інтелектом, технологіями розпізнавання облич, не адресує небезпек від соцмереж тощо. Фактично документ не встановлює і жорстких правил поводження з біометричними або іншими чутливими видами даних. Як наслідок, незважаючи на досить детальну політику, усе впирається в її застосування в різноманітних контекстах.

Чи є політики ефективними на практиці? У 2019 році Драгана Каурін підготувала дослідження про політики щодо захисту персональних даних міжнародних організацій та їх застосування до реальних сценаріїв. Чи не ключове місце в цьому дослідженні було відведене саме УВКБ ООН. Його результати видаються не надто втішними, щонайменше відповідно до відгуків осіб, які отримували гуманітарну допомогу й реєструвалися як біженці.

Так, організації, які надавали гуманітарну допомогу й асистували в реєстрації осіб як біженців, часто запитували надмірні обсяги даних: наприклад, фіксували інформацію про сексуальну орієнтацію, освіту чи етнічну приналежність, наявність невиліковних хвороб (на кшталт раку чи СНІДу). Часто збирали й біометричні дані, як-от відбитки пальців, відбиток сітківки ока чи звичайні фотографії особи. Одним з найпоширеніших виправдань є те, що це допомагає запобігти шахрайству й подвійному наданню допомоги в одні руки. Водночас дослідження показують, що як відбитки пальців, так і розпізнавання облич можуть бути неточними, адже системи часто віддзеркалюють інституційну дискримінацію. Понад те, під час надання допомоги біженцям з М'янми у 2018 році УВКБ ООН створювало профайли на осіб, яким надавало допомогу. Одним з критеріїв була етнічна приналежність, що створювало ризики репатріації етнічної спільноти рогінья через дискримінаційно налаштовану владу Бангладеш, куди громадяни М'янми втікали від геноциду. Окрім того, під

час допомоги сирійським біженцям у Лівані у 2014 році, УВКБ ООН стикнулося з проблемою вимоги ліванським урядом доступу до бази даних біженців. Тобто збір надмірної кількості даних не лише непропорційний, а й часто небезпечний для отримувачів гуманітарної допомоги, адже уряди сусідніх держав можуть бути налаштовані досить вороже.

На додаток, окрім простого збору даних, проблема часто полягає і у верифікації інформації. Зокрема, якщо допомога першочергово призначена для осіб, які пережили сексуальне чи фізичне насилля, тортури чи нелюдське поводження, для вагітних жінок чи осіб з хронічними захворюваннями, організації вимагали підтвердити цей статус. Оскільки біженці часто не мали документів про стан здоров'я чи доказів того, що вони постраждали від злочинів, процедура сама собою була дуже травматичною для таких осіб. Наприклад, Каурін згадує випадок, коли 6 500 біженців у Мавританії не мали доступу до їжі, медичної допомоги та інших важливих сервісів через те, що система неправильно розпізнала їх.

Зрештою, незважаючи на те, що політика УВКБ ООН містить дуже деталізоване пояснення мети використання даних, біженці зазначають, що на практиці надавачі допомоги нічого не пояснювали. Тобто політика часто декларативна. Так, сирійські біженці в Греції не могли отримати адекватних роз'яснень щодо причин зняття відбитків пальців, тоді як єдиною відповіддю було те, що це «нормальна процедура». Як наслідок, самі лише формулювання політик, очевидно, недостатні для того, щоб ефективно захищати персональні дані отримувачів гуманітарної допомоги.

Хоча в Україні подібних випадків не було виявлено переважно через більш толерантне ставлення європейців до біженців та кращої координації процесів надання гуманітарної допомоги, надмірний збір даних усе ще трапляється, адже біометрична ідентифікація є частиною загального механізму встановлення особи отримувача допомоги. Тобто в разі витоку даних УВКБ ООН ризикує стикнутися з проблемами використання зібраних даних зловмисниками, у тому числі з держави-агресора.

ЮНІСЕФ. Організація багато працює «в полі», безпосередньо бере участь у гуманітарних місіях, оперуючи великими масивами персональних даних, а тому потребує деталізованих політик щодо захисту даних. Наприклад, в Україні ЮНІСЕФ надає грошову допомогу в межах проєкту «Спільно», який передбачає отримання базового набору персональних даних для ідентифікації особи та її соціального статусу.

ЮНІСЕФ має окрему Політику щодо захисту персональних даних від 2020 року, досить стислий документ, що викладає основні принципи роботи з такою інформацією. Важливі елементи політики:

- **принципи** (легітимні підстави для обробки даних, дотримання мети обробки даних, достатність даних і їх якість, необхідність і пропорційність, безпека, обмеженість періоду зберігання даних);
- **повідомлення про обробку даних;**
- **права суб'єкта** (доступ до інформації, право виправляти дані, заперечувати проти обробки, вимагати видалення, право заперечувати проти автоматизованого ухвалення рішень);
- **передача даних третім особам** (без жодної деталізації);
- **відповідальність і надзвичайні заходи** (у контекстах, коли неможливо забезпечити дотримання політик у вигляді, у якому вони представлені, і процедура для відступів від зобов'язань);
- **нагляд за дотриманням політик захисту даних** (з деталізованими процедурами);
- **найкращі інтереси дитини** (ЮНІСЕФ зазначає, що обробка персональних даних у жодному разі не має порушувати інтересів дитини).

Серед пунктів, які, очевидно, викликають занепокоєння, варто відзначити те, що серед *«легітимних інтересів та підстав»* для обробки даних ЮНІСЕФ зазначає *«інші інтереси»* — категорію, яка може трактуватися дуже широко. З іншого боку, період зберігання даних обмежується 10 роками, і в разі перевищення цього періоду ЮНІСЕФ має додатково обґрунтувати необхідність подальшого зберігання даних.

Зрештою, ЮНІСЕФ розробила розширені Керівництва щодо приватності, етики і захисту даних, які детально описують усі процедури й процеси, яких необхідно дотримуватися при наданні гуманітарної допомоги.

Як помітно, політика досить загальна і радше рамкова, що передбачає багато практичних викликів при її застосуванні. Зокрема, у питаннях оцінювання добровільності й поінформованості згоди, автоматизованої обробки даних тощо. Часто при зборі даних виникають проблема, коли пояснення мети їх збору (у таких обсягах, як їх збирають) і подальшої долі зібраної інформації не зрозумілі.

Окрім того, в Україні ЮНІСЕФ навіть став фігурантом скандалу навколо нехтування положеннями українського законодавства про захист даних організацією. Це своєю чергою змусило багатьох насторожено ставитися до отримання допомоги в міжнародних центрах. Наприклад, минулоріч виник скандал з приводу неправомірного збору персональних даних ЮНІСЕФ у межах програми грошової допомоги «Спільно», яка розрахована на виділення коштів багатодітним родинам чи родинам з дітьми, які мають інвалідність. Логічним у цьому випадку було збирання інформації про наявність у родині дітей та стан їх здоров'я. Водночас блогер Сергій Гула у своєму відео зазначав, що ЮНІСЕФ не отримує дозволу на обробку персональних даних, неконтрольовано передає їх третім особам і не впроваджує жодних гарантій безпеки, порушуючи Закон України «Про захист персональних даних».

Як виявилося, жодних порушень з боку ЮНІСЕФ не було. Про це у своєму дослідженні розповіли українські фактчекери з VoxCheck. Зокрема, вони перевірили правила обробки персональних даних, якими керується ЮНІСЕФ, а також особу адвоката, який поширював інформацію про незаконний збір персональних даних. З'ясувалося, що він і раніше робив неправдиві заяви в контексті пандемії та вакцинації, тому поширена дезінформація не стала першим епізодом. Проте такі акції досить небезпечні, адже вони підривають довіру до міжнародних інституцій і сприяють тому, що особи, які потребують допомоги, бояться звернутися по неї через страх шахрайства й порушення прав.

Утім, це не означає, що порушень з боку ЮНІСЕФ не траплялося взагалі. Так, у 2019 році збій у системі навчальних онлайн-курсів дозволив дізнатися персональні дані близько 8 200 користувачів. Витік даних передбачав поширення імен, адрес пошти, віку, статі, організації та навіть видів договорів, укладених з особою. З позитивного — ЮНІСЕФ швидко визнав проблему й навіть пояснив, що витік даних був спричинений технічною помилкою одного зі співробітників.

Як бачимо, навіть інституції ООН не є ідеальними в питаннях захисту даних, і тут багато чого залежить саме від людського фактора. Водночас слід дуже обережно ставитися до інформації, яка ширяться в мережі стосовно порушень правил поводження з персональними даними. Інакше дезінформація ризикує підірвати репутацію гуманітарних організацій і призвести до неотримання допомоги людьми, які її справді потребують.

Європейська рада у справах біженців і вигнанців. Для порівняння з політиками організацій у структурі ООН варто розглянути регіональну інституцію. Європейська рада видається найбільш наближеною до українського контексту, а тому найрелевантнішою установою, яка надає гуманітарну допомогу. Ця організація, як і багато інших, розробила окремі політики щодо захисту даних, адаптовані до гуманітарних контекстів.

Правила роботи з персональними даними в Європейській раді називаються «Захист даних: політика приватності і керівництва», вони досить коротко та чітко викладені:

- **принципи** (мінімізації даних, легітимних підстав для обробки даних);
- **поширення інформації третім особам** (зокрема, розкривається інформація про те, з якими третіми особами є постійні технічні договори, як-от Google, Microsoft тощо);
- окрема **особа, відповідальна за захист даних;**
- **реєстрація активностей,** що передбачають обробку даних;
- **повідомлення про порушення;**
- **примат GDPR** над іншими регуляціями та постійні відсилки до його положень.

Показово, що на відміну від інституцій ООН Європейська рада має вичерпний і чіткий перелік підстав для збору і обробки даних, а категорія «суспільного інтересу» є розкритою і супроводжується обов'язком Європейської ради збалансувати інтереси й забезпечити дотримання принципу необхідності та пропорційності. Водночас у публічній політиці бракує інформації про те, які права мають суб'єкти та яким чином їм слід звертатися до організації для реалізації таких прав.

Важливо також, що Європейська рада діє як одна з інституцій ЄС. Відповідно на неї поширюються вимоги щодо захисту персональних даних, у тому числі і в політиках вебсайтів, які створюють органи ЄС. На практиці це означає, що вебсайти мають містити попередження про використання кукіз та подібну інформацію про дані, які вони збирають про особу, ще до того, як мова заходить про надання допомоги чи іншу гуманітарну дію. Водночас Європейська рада не фігурувала в скандальних історіях про порушення порядку захисту даних, що дає надію на досить серйозний юридичний і технічний захист інформації, отриманої під час надання гуманітарної допомоги.

Окрім проаналізованих організацій, робота яких найактуальніша в контексті збройної агресії Росії в Україні, існують й інший гуманітарні організації, як-от Світова продовольча програма ООН (має політики аж на 130 сторінок), Офіс ООН з координації гуманітарних питань, Міжнародна організація з питань міграції, Генеральний директорат Європейської комісії з питань цивільного захисту та гуманітарної допомоги та багато інших профільних органів. Більшість з них мають політики щодо захисту даних, рівень деталізації яких варіює залежно від віку такого документа і контекстів, з якими організації стикалися в роботі, утім, загальною проблемою залишається застосування писаних принципів і правил на практиці.

Міжнародні неурядові організації

Міжнародні неурядові організації, на відміну від урядових, більш вільні в тому, які засоби використовувати для збору персональних даних під час надання гуманітарної допомоги. Ба більше, вони гнучкіші і в процесах звітування і нагляду, а також формування органів, які займаються наданням допомоги. З іншого боку, перед неурядовими організаціями часто постає питання звітування перед донорськими організаціями за надану гуманітарну допомогу. Так, вони мають повідомити кількість осіб, які її отримали, задоволення формальних вимог щодо надання допомоги (наприклад, факт того, що сім'я є багатодітною чи що особа має проблеми зі здоров'ям тощо). Це своєю чергою породжує нову категорію проблем.

Здавалося б, міжнародні організації, які працюють з настільки чутливими питаннями і чиї офіси розташовані в демократичних країнах, спроможні забезпечити один з найвищих рівнів захисту для зібраних даних. Утім, на практиці все не так просто. Наприклад, у січні 2022 року, напередодні повномасштабного вторгнення Росії в Україну, відбувся масовий

витік даних з бази МКЧХ (дані близько 515 000 осіб), що спричинило перебої в гуманітарних операціях. І це лише один приклад того, наскільки незахищеними є неурядові організації. Загалом статистика показує, що близько двох третин неурядових організацій у різний час були об'єктом хакерських атак чи витоків даних, а також не приділяють належної уваги оцінюванню кібербезпекових ризиків. Тобто викликів перед глобальними міжнародними неурядовими організаціями наразі постає чимало. І єдине питання, чи здатні вони з цими викликами впоратися так, щоб не наразити отримувачів допомоги на ще більшу небезпеку?

МКЧХ і Міжнародна федерація Товариств Червоного Хреста і Червоного Півмісяця (далі — МФЧХіЧП). На відміну від поширеної думки, МКЧХ і МФЧХіЧП не є однією організацією. Вони мають дещо різні мандати, порядок ухвалення рішень і, що важливо в межах нашої теми, різні політики захисту персональних даних. Утім, оскільки ці дві інституції досить сильно пов'язані між собою, їх усе ж варто оцінити порівнюючи, щоб зрозуміти, наскільки політики можуть бути неузгодженими між собою навіть у «сестринських» організаціях.

Правила захисту персональних даних **МКЧХ**	Політика щодо захисту персональних даних **МФЧХіЧП**
Обсяг і деталізація положень у правилах нагадують структуру документів ООН, тож вони досить всеохопні: ■ **принципи** (легітимні підстави для обробки даних, прозорість, дотримання мети обробки даних, достатність даних і їх якість, архівування чи видалення даних, які більше не є актуальними); ■ **права суб'єкта** (доступ до інформації, право виправляти дані, заперечувати проти обробки, вимагати видалення, право не отримувати рішень, які базуються на профайлінгу); ■ **можливість відступу від обов'язків у надзвичайних ситуаціях;** ■ **модель захисту даних за дизайном і за замовчуванням;** ■ **оцінювання впливу на персональні дані** (організація має оцінювати політики роботи з даними контекстуально і так швидко, як це можливо); ■ **документування обробки даних;** ■ **кооперація з наглядовими органами** (національного чи регіонального рівня); ■ **повідомлення про порушення** і відповідальність; ■ **передача даних третім особам** (у тому числі органам правопорядку, а також доступ для генеалогічних та адміністративних досліджень); ■ **офіс і комісія із захисту даних** (як наглядові органи МКЧХ, які ухвалюють рішення про практики роботи з персональними даними й розглядають випадки порушень відповідно).	Сама політика досить коротка та стисла, утім, загальна за своєю природою. Зокрема, вона містить декілька розділів, що уточнюють правила роботи з даними: ■ **принципи** (наявність легітимних підстав для обробки даних, доступ до інформації, уточнення мети обробки, мінімізація даних, зберігання даних не довше, ніж необхідно, безпека та конфіденційність даних); ■ **права суб'єкта** (доступ до інформації, право виправляти дані, заперечувати проти обробки, вимагати видалення, отримувати своєчасну та зрозумілу відповідь на запити); ■ **оцінювання впливу на персональні дані** (організація має оцінювати нові технології, переглядати рішення автоматизованих систем, оцінювати контекстуальні ризики в умовах застосування масового стеження); ■ **повідомлення про порушення і відповідальність;** ■ **передача даних третім особам** (у тому числі органам правопорядку).

Правила захисту персональних даних МКЧХ	Політика щодо захисту персональних даних МФЧХіЧП
У формулюваннях Правил, утім, наявні такі підстави обробки даних, як «переслідування легітимних цілей МКЧХ, якщо це не шкодить правам суб'єкта» та «дотримання правових вимог / обов'язків», що може передбачати фактично будь-яку підставу, наявну в статуті МКЧХ, його договорах з іншими суб'єктами чи інших внутрішніх документах. Окрім того, у разі діяльності МКЧХ в авторитарних країнах може виникнути дилема: надавати персональні дані авторитарним урядам чи не дотримуватися місцевого законодавства. Наразі Правила передбачають саме дотримання законодавства без жодних винятків і застережень, що може призвести до порушень прав людини. Також однією із цілей обробки даних є «побудова поваги до гуманітарного права», що викликає досить багато питань у контексті персональних даних (зокрема, для тренінгів і круглих столів можна використовувати анонімізовані й псевдонімізовані дані). Зрештою, замість видалення даних Правила передбачають архівування у випадках, коли це корисно для статистики, історичних чи наукових цілей, тобто фактично в будь-якій ситуації. Це своєю чергою створює певні ризики, адже цифрові архіви все ще можуть ставати об'єктами хакерських атак чи зламів. Водночас МКЧХ має скорочену та спрощену версію Правил на власному вебсайті, що детально пояснює права суб'єктів і дозволяє їм зрозуміти, що відбувається із зібраними персональними даними та як звернутися до МКЧХ із запитом щодо даних. Це, безперечно, позитивний крок, адже полегшує роз'яснення, а також відповідає принципу прозорості.	У формулюваннях Політики непокоїть наявність таких підстав для обробки даних, як «переслідування легітимних цілей Федерації» та «виконання завдань у суспільному інтересі», що може передбачати фактично будь-яку підставу, наявну в статуті МФЧХіЧП, договорах Федерації з іншими суб'єктами чи інших внутрішніх документах. Це може стати небезпечним, особливо коли організація не до кінця усвідомлює контекст роботи і, наприклад, співпрацює з урядом, який може вдаватися до порушень прав людини. Також бракує деталізації згоди особи, умов визнання її валідною, умов автоматичного видалення інформації після спливу терміну зберігання даних тощо. Водночас організація має декілька окремих керівних документів для роботи із системами передачі даних чи коштів. Так, Практичне керівництво щодо захисту даних при наданні допомоги у готівці та формі ваучерів передбачає більш деталізовані правила для надання допомоги, які ґрунтуються на форматі й доступних способах надання тако допомоги.

Як і у випадку з інституціями ООН та іншими міжнародними організаціями, МКЧХ і МФЧХіЧП мають загальні політики загального, які суттєво залежать від практичного застосування. Тож ключове питання: чи ці гуманітарні організації на практиці такі ж добросовісні, як у писаних політиках?

З цього приводу щонайменше виникають сумніви, адже МКЧХ достатньо активно збирає біометричні дані отримувачів гуманітарної та інших видів допомоги. Наприклад, організація використовує програмне забезпечення на вебсайті «Trace the Face» для розпізнавання облич біженців, шукачів притулку й отримувачів гуманітарної допомоги з метою відновлення сімейних зв'язків. Вебсайт сам собою не надає жодної інформації про те, яким чином обробляються і зберігаються персональні дані ані з правової, ані з технічної

точки зору. Окрім того, на вебсайті зберігаються зображення віком більше ніж 10 років, тож не відомо, чи до них також застосовують технологію розпізнавання облич, якщо так, чи було на це отримано дозвіл при зборі даних.

Уже згадувався випадок хакерської атаки на базу даних МКЧХ, під час якої близько 515 000 осіб опинилися в дуже вразливому становищі. З технічної точки зору це вказало на прогалини в системі захисту, а ще на неможливість повністю убезпечити дані проти хакерських атак та зовнішніх загроз. З позитивного — МКЧХ принаймні вчасно скомунікував про витік даних, повідомивши про кількість втраченої інформації та тих, кого вона стосувалася. Комітет навіть поширив деталі атаки та її наслідків. Водночас після інциденту Уповноважена Верховної Ради України з прав людини звернулася до МКЧХ з вимогою повідомити про порядок захисту даних.

International Rescue Committee (далі — IRC). Не всі організації мають детальні політики щодо захисту даних. У деяких випадках їх навіть важко знайти за допомогою вільного пошуку у Google. І IRC є однією з них.

Політики у сфері захисту даних IRC різняться залежно від регіону: вебсайт організації надає можливість обрати одну з кількох опцій (США, Велика Британія, Німеччина, Швеція, ЄС та Корея). У цьому аналізі ми зосередимося на політиці, яка вважається глобальною, — Політиці приватності. На відміну від політик багатьох інших організацій, цей документ розміщений в окремому розділі вебсайту, а тому може регулярно оновлюватися (читачі можуть не помічати цього). Утім, структура документа досить зрозуміла:

- **перелік даних, що збираються** (зокрема, ідеться про куків, дані, необхідні для співпраці з IRC, а також інформацію, що надається для підписки на оновлення);
- **передача даних третім особам** (провайдерам, благодійним організаціям, у межах судового провадження, у виняткових випадках — передача даних у бізнес-цілях);
- **захист даних** (технічні протоколи);
- **кукіз** (з деталізацією мети, способу збору та поясненнями технічної сторони процесу налаштування кукіз на вебсайті);
- **посилання на GDPR;**
- **приватність дітей** (особливі правила).

Окрім політики для користування вебсайтом, також існує Організаційна політика. Вона більш застосовна до процесу надання гуманітарної допомоги. Утім, жодних деталізацій щодо захисту даних, прав суб'єктів чи можливості видалення даних вона не містить:

- **посилання на GDPR** і загальний обов'язок поваги до приватності;
- **невичерпний перелік даних, які збираються;**
- **заборона вільного поширення біометричних даних біженців** без згоди Бюро з питань населення, біженців та мігрантів США

Примітно, що в Політиці, яка стосується безпосередньо «роботи в полі», відсутні будь-які деталізації прав і можливостей суб'єктів надсилати запити на видалення чи коригування даних, заперечувати проти обробки даних тощо. Також відсутні загальні принципи, якими керується організація при роботі з даними. Це досить небезпечна тенденція, особливо з того погляду, що організація позиціонує себе як лідера у сфері надання гуманітарної допомоги. Водночас позитивним аспектом політики є ілюстративність: наведені модельні ситуації, які демонструють, як IRC відповідатиме на ті чи інші запити громадськості.

З позитивних аспектів, IRC використовує систему «Box Shield», яка забезпечує посилений

захист персональних даних за допомогою додаткової системи аутентифікації. Загалом це позитивний крок, адже дозволяє запобігати витокам даних. З іншого боку, використання сторонньої системи свідчить про те, що IRC не має власних розробок на цьому полі, тобто послуговується зовнішніми ресурсами.

Save the Children (далі — SCI).

Організація досить вузькоспеціалізована і працює безпосередньо з вразливими групами й чутливою інформацією. Відповідно це сприяє створенню особливого порядку роботи з персональними даними.

Політика щодо захисту даних — це невеликий структурований файл, який окреслює основні принципи роботи з персональними даними з акцентом на чутливості даних, пов'язаних з дітьми (зокрема, **найкращі інтереси дитини**):

- **посилання на GDPR** (включно з існуванням особи, відповідальною за захист даних);
- **принципи** (легітимні підстави для обробки даних, прозорість, дотримання мети обробки даних, мінімізація даних, якість даних, архівування чи видалення даних, які більше не актуальні, конфіденційність і відповідальність);
- **тренінги для персоналу щодо захисту даних** (кожні 12 місяців);
- **згода на обробку даних** (активна, усвідомлена та поінформована згода, наявність батьківської згоди для дітей (осіб віком до 18 років);
- **прозорість і інформування** (кількість даних, мета збору, правова підстава, тривалість зберігання даних, передача даних третім особам);
- **оцінювання впливу на персональні дані** (приватність за замовчуванням, організація має оцінювати нові технології, особливо щодо збору й обробки чутливих даних);
- **права суб'єкта** (доступ до інформації, право виправляти дані, заперечувати проти обробки, вимагати видалення, отримувати своєчасну та зрозумілу відповідь на запити, право на забуття);
- **передача даних третім особам** (у тому числі міжнародні трансфери даних);
- **безпека даних** (адміністративні й технічні заходи);
- **повідомлення про порушення і відповідальність.**

У формулюваннях Політики непокоїть наявність таких підстав для обробки даних, як «переслідування легітимних цілей SCI» та «дотримання правових вимог / обов'язків», що може передбачати фактично будь-яку підставу, наявну в статуті, договорах з іншими суб'єктами чи інших внутрішніх документах. Це може бути небезпечно, особливо коли організація не до кінця усвідомлює контекст роботи і, наприклад, співпрацює з урядом, який вдається до порушень прав людини.

Водночас SCI має окремі гайдлайни, як отримувати згоду на обробку даних, повідомлення про порушення, кібербезпеку та інші процедурні аспекти. Скорочена версія політик приватності викладена в доступній формі на вебсайті організації з посиланнями на основні права суб'єктів, категорії даних й активності, для яких дані збираються. Окрім того, організація має окремі вебсайти та окремі політики для регіональних осередків, як-от США.

Утім, гарно пропрацьовані політики не означають, що організація ніколи не була об'єктом атак чи має ідеальну історію захисту даних. Так, у 2018 році шахраї, представившись одним зі співробітників, підробили інвойси та вкрали близько 1 000 000 доларів з рахунків організації. За схожою схемою шахраї могли отримати й доступ до персональних даних. Іншим випадком стали безпекові прогалини. У липні 2020 року відбулася кібератака на

одного з постачальників програмного забезпечення SCI, про що організація повідомила на своєму вебсайті. На жаль, витік даних зачепив й отримувачів допомоги від SCI, у тому числі дані про вік, стать й історію залучення дітей до програм організації. Це свідчить про відносну неспроможність організації спрогнозувати кібервиклики, особливо коли вона вдається до послуг третіх осіб у питаннях зберігання даних на серверах тощо.

Окрім детально проаналізованих компаній, у межах дослідження ми також розглядали й опитували такі неурядові організації, як Medicos del Mundo, HelpAge International, Triangle Génération Humanitaire, Premiere Urgence Internationale, Handicap International і Red Rose CSP. За загальними стандартами більшість політик досить схожі між собою в організацій, які працюють у сфері надання гуманітарної допомоги. Різниця помітна переважно в питаннях, які стосуються їх фокусів роботи: вразливі меншини, особи з інвалідністю, діти тощо. Як наслідок, превалювання чутливої категорії даних може робити політики приватності організацій заточеними під розв'язання конкретних проблем. Утім, на практиці безпекові проблеми і відносна технічна незахищеність досить поширене явище.

Як помітно з досліджень, неурядові організації часто не мають належної технічної експертизи, а також людських, фінансових та/або технічних ресурсів, щоб адекватно передбачити технічні загрози (як-от зливи даних, хакерські атаки чи недбалість співробітників) і запобігти їм. Як наслідок, для неурядових організацій характерне скоріше реактивний, ніж проактивний підхід у протидії кіберзагрозам. Це своєю чергою дуже небезпечно в гуманітарному контексті, адже у випадку зламів баз даних, витоків інформації чи технічних несправностей відновити попередній стан речей практично неможливо — персональні дані вже будуть у руках зловмисників. Тому гуманітарним організаціям слід звертати особливу увагу на запобігання загрозам заздалегідь, ніж на реагування на них постфактум.

Іноземні місцеві організації

Місцеві організації з транскордонними проєктами (гуманітарна допомога за кордоном) мають свої особливості роботи з персональними даними. Вони повинні створювати політики відповідно до законодавства держави, у якій вони зареєстровані, і держави, де вони надають допомогу. Теоретично це просто, на практиці ж законодавство надто загальне, і все залежить від того, як сформульовані внутрішні політики, де зберігаються дані та кому вони в результаті можуть передаватися. З огляду на те, що суспільна увага до таких організацій менш прискіплива порівняно з МКЧХ чи іншими «гігантами» гуманітарної сфери, виникає питання: чи настільки ж добросовісно організації дотримуються правил роботи з даними? Наприклад, в Італії гуманітарні організації збирали дані про сексуальну орієнтацію біженця при наданні допомоги. Мету збору таких даних не повідомляли, що спричинило ще більше дискомфорту для особи, яка і без того перебуває в складних життєвих обставинах (не кажучи вже про принцип мінімізації даних).

People in Need (далі — PIN) (Чехія). Чеська організація, яка надає допомогу та юридичну підтримку в багатьох регіонах, включно з Україною. PIN належить до організацій, які працюють «у полі», тобто збирають персональні дані під час надання допомоги. Окрім того, PIN є однією з небагатьох організацій, які відреагували на опитування від УМДПЛ, роз'яснивши, яким чином вони зберігають й охороняють персональні дані, якими документами керуються і які стандарти застосовують. З важливого, PIN вказала два документи, на яких ґрунтується їхня політика, Довідник МКЧХ щодо захисту даних під час гуманітарних акцій і GDPR. У відповідь на запит УМДПЛ щодо уточнення практик захисту даних, PIN наголосила:

> ***«Основним принципом усіх політик PIN щодо захисту даних є те, що наша діяльність, якщо вона включає роботу з персональними даними бенефіціарів PIN, здійснюється з професійною ретельністю, прозоро і так, щоб поважати права особи з точки зору захисту її персональних даних. Вимоги всіх внутрішніх інструкцій повинні застосовуватися в максимально можливому обсязі також***

у випадках співпраці з іншими суб'єктами (організаціями, які контактують з будь-якими персональними даними PIN або бенефіціарів PIN на підставі договірних відносин)».

Це означає, що аналогічні політики застосовуються і до третіх осіб, які кооперуються з PIN для надання гуманітарної допомоги: її місцевими партнерами чи навпаки — парасольковими організаціями на міжнародному рівні. Це позитивно і в контексті надання допомоги в Україні, яка передбачає співпрацю з місцевими організаціями.

Політика щодо захисту даних доступна в онлайн-версії і стосується дуже загальних правил поводження з інформацією. Зокрема, вона містить:

- **посилання на GDPR** (включно з існуванням особи, відповідальної за захист даних);
- **принципи** (легітимні підстави для обробки даних, дотримання мети обробки даних, необхідність і пропорційність);
- **види даних,** які збираються найчастіше (кукіз, дані про донорів, дані отримувачів допомоги та соціальних сервісів, дані від осіб, які підписуються на дайджести);
- **права суб'єкта** (доступ до інформації, пояснення мети й долі зібраних даних; право виправляти дані, заперечувати проти їх обробки, вимагати видалення, отримувати своєчасну та технічно зрозумілу відповідь на запити, право на забуття).

На додаток, на вебсайті PIN є окремий список тих, хто може отримувати інформацію відповідно до положення про зберігання даних про і для донорів. Безперечно, позитивно, що політика є стислою та зрозумілою для пересічної особи. Водночас дуже багато аспектів, важливих для захисту даних, не охоплені цією політикою, а розширена версія на вебсайті PIN не розміщена. Наприклад, бракує інформації про оцінювання впливу політик і практик на захист даних, деталізації передачі даних третім особам, повідомлення про порушення і приватність.

Як уже зазначалося, медійних випадків, пов'язаних з витоками даних з баз даних PIN, немає. Водночас слід усвідомлювати, що організація може легко опинитися в переліку тих, чиї дані були об'єктом витоку під час зламу бази даних отримувачів допомоги від уряду США. Утім, жодних публічних повідомлень про це не надходило, тож можна презюмувати, що PIN пощастило уникнути проблемних випадків з безпекою даних.

ACTED (Франція). Французька організація, яка переважно працює «в полі» та безпосередньо надає гуманітарну допомогу постраждалим від війни чи інших лих. ACTED працює і в Україні, забезпечуючи населення найбільш вразливих регіонів харчовими продуктами, одягом та іншими засобами першої потреби в умовах збройного конфлікту. Організація також допомагає біженцям і прогнозує розвиток гуманітарної ситуації на основі зібраних даних.

Політика щодо захисту даних ACTED дуже добре структурована, утім, трохи не схожа на міжнародні неурядові чи міжурядові організації. Утім, не можна сказати, що це робить її гіршою, скоріше навпаки. Організації вдалося вкласти в 10 сторінок усю інформацію, на яку деякі інші інституції потребували 40 сторінок:

- **мета та сфера дії** Політики (у тому числі застосовна до партнерських організацій);
- **види даних,** які збираються найчастіше (ім'я, адреса, засоби зв'язку, номер паспорта, дата і місце народження, інформація про родичів, геолокація, бізнес-контакти, відбитки пальців);
- **застосовне регулювання** (французьке законодавство, GDPR і національні

законодавства країн, у яких діє ACTED);

- **принципи** (легітимні підстави для обробки даних, дотримання мети обробки даних, прозорість, необхідність і пропорційність, конфіденційність і безпека даних, якість і точність даних);
- **обробка даних** (згода, наявність легітимного інтересу, телекомунікації та інтернет — технічні вимоги до використання засобів комунікації у роботі з гуманітарними питаннями);
- **права суб'єкта** (доступ до інформації, право запитувати видалення даних і заперечувати проти їх обробки);
- **передача даних** (у тому числі в межах співпраці з органами правопорядку, але за умови погодження передачі даних відповідальною за захист даних особою всередині організації);
- **вимоги до відповідей на запити щодо даних** (своєчасність, зрозумілість, чіткість і повнота, застосовність як до запитів від осіб, так і від партнерських організацій);
- **конфіденційність та безпека** (у тому числі технічна);
- **повідомлення про порушення і відповідальність**

Це одна з небагатьох політик, яка прямо вказує на те, що вона застосовна до біометричних даних (відбитків пальців). Хоча, на жаль, мета їх збору та обробки не уточнена. Загалом політика ACTED є однією з найдосконаліших з точки зору поводження з даними й процесів передачі й обробки даних з дотриманням усіх необхідних гарантій. До того ж вона сформульована просто й зрозуміло, стисла й доступна для пересічного читача.

Окрім Політики щодо захисту даних, ACTED має інші спеціалізовані політики, як-от щодо захисту дітей, запобігання сексуальним домаганням і злочинам у сексуальній сфері тощо. Деякі безпосередньо стосуються захисту чутливих даних і важливі, особливо з огляду на те, що ACTED працює з вразливими групами «в полі», діючи в небезпечних контекстах та оперуючи чутливою інформацією. Окрема політика також стосується захисту даних під час використання вебсайту. Утім, вона «захована» серед інших правил користування вебсайтом, і знайти її не так легко.

Випадків, пов'язаних з витоками даних з її баз даних, не виявлено. Водночас, як і багато інших представників громадського сектору, організація могла опинитися в переліку тих, чиї дані були об'єктом витоку під час зламу бази даних отримувачів допомоги від США. Слід зазначити, що в разі подібних інцидентів важливо, щоб організація належно комунікувала про наявність порушень режиму захисту даних.

IMPACT (Швейцарія). Організація готує аналітичні звіти про порушення гуманітарного права та вплив збройних конфліктів на права людини, моніторить середовище щодо гуманітарних потреб і розробляє плани надання гуманітарної допомоги, у тому числі і в контексті російської збройної агресії в Україні. IMPACT цікава для дослідження, адже на відміну від PIN та ACTED вона працює з персональними даними як третя особа, що отримала їх від інших організацій, які безпосередньо збирали дані. Це означає, що і політики захисту даних мають відповідати міжнародним стандартам.

Політика щодо захисту даних IMPACT трохи відрізняється за структурою від політик організацій, які працюють «у полі», що логічно, адже мета діяльності та способи роботи з інформацією кардинально інші. Єдиним винятком є ACTED, із чиєю політикою вона дуже схожа, адже організації перебувають у тісному партнерстві. Тому структура й акценти політики IMPACT виглядають схожими на Політику ACTED:

- **мета та сфера дії** Політики (у тому числі застосовна до партнерських організацій);
- **види даних,** які збираються найчастіше (ім'я, адреса, засоби зв'язку, номер паспорта, дата і місце народження, інформація про родичів, геолокація, бізнес-контакти, відбитки пальців);
- **застосовне регулювання** (швейцарське законодавство та Політики ACTED щодо захисту прав дитини);
- **принципи** (легітимні підстави для обробки даних, дотримання мети обробки даних, прозорість, необхідність і пропорційність, конфіденційність і безпека даних, якість і точність даних);
- **обробка даних** (згода, наявність легітимного інтересу, телекомунікації та інтернет — технічні вимоги до використання засобів комунікацій у роботі з гуманітарними питаннями);
- **права суб'єкта** (доступ до інформації, право запитувати видалення даних і заперечувати проти їх обробки);
- **передача даних** (у тому числі в межах співпраці з органами правопорядку, але за умови погодження передачі даних відповідальною за захист даних особою всередині організації);
- **вимоги до відповідей на запити щодо даних** (своєчасність, зрозумілість, чіткість і повнота, застосовність як до запитів від осіб, так і від партнерських організацій);
- **конфіденційність та безпека** (у тому числі технічна);
- **повідомлення про порушення і відповідальність.**

Цей документ прямо вказує на застосовність до біометричних даних (відбитків пальців), хоч і (знову ж таки) без уточнення мети. У решті питань Політика IMPACT (як дзеркальна до Політики ACTED) є однією з найдосконаліших з точки зору поводження з даними й процесів передачі й обробки даних з дотриманням усіх необхідних гарантій.

Окрім Політики щодо захисту даних, IMPACT має багато інших більш спеціалізованих політик, як-от політику щодо захисту дітей, запобігання сексуальним домаганням чи злочинам у сексуальній сфері тощо. Деякі з них безпосередньо стосуються захисту чутливих даних і важливі, особливо з огляду на те, що IMPACT здійснює моніторинг і планування акцій з надання гуманітарної допомоги вразливим групам. Окрема політика також розроблена для повідомлення про правила захисту даних на вебсайті та під час його використання.

З огляду на те, що IMPACT не працює з персональними даними напряму, а скоріше отримує їх від інших організацій для статистики, прогнозування та досліджень, логічно, що організації нема у списку першочергових цілей для хакерських атак. Як наслідок, випадків, пов'язаних з витоками даних з її баз даних, не виявлено. Водночас, як і багато інших представників громадського сектору, організація могла опинитися в переліку тих, чиї дані були об'єктом витоку під час зламу бази даних отримувачів допомоги від США. Слід зазначити, що в разі подібних інцидентів важливо, щоб організація вчасно й належно комунікувала про наявність порушень режиму захисту даних.

Окрім того, багато інших місцевих організацій мають дуже деталізовані політики захисту даних. Наприклад, Norwegian Refugee Council має дуже детальну та добре структуровану політику, яка охоплює як юридичні, так і деякі технічні питання. Cyprus Refugee Council діє схожим чином, маючи деталізовану й структуровану політику щодо захисту персональних даних. Аналогічною є політика Danish Refugee Council, яка також має ще й перелік додаткових керівництв для внутрішнього користування, які регулюють особливі аспекти роботи з даними. Окрім того, Danish Refugee Council має спеціальну систему, яка орієнтована на прогнозування, наприклад, примусових переселень і криз біженців на найближчі 1–3 роки,

що передбачає обробку персональних даних у великих масштабах для цілей, які пов'язані з гуманітарною допомогою побічно. Важливо, що такі системи згодом можуть «мігрувати» до держави та використовуватися для запобігання імміграції, напливам біженців чи навіть вчиняти злочини проти людяності, якщо режими схильні до авторитарних практик. Тому з трансфером подібних технологій слід бути вкрай обережними.

Досить детальну політику має данська організація Bevar Ukraine, створена спеціально для допомоги постраждалим від російської агресії в Україні (важливо, що політика доступна українською). Набагато менш детальні політики в Arche Nova Organisation та Equilibrium, які до того ж ще й досить важко знайти через базову навігацію на вебсайті та за допомогою пошуковика Google. Зрештою, відносно нові організації, як-от Geneva Call узагалі не мають політики приватності в публічному доступі. Це може свідчити про одне з двох: або організація взагалі не має кодифікованих політик, тому отримувачі гуманітарної допомоги не можуть ознайомитися з принципами роботи з даними, їхніми правами та рівнем захисту від несанкціонованого доступу, або вони не оприлюднені на вебсайті (що фактично призводить до тих самих наслідків).

Тобто порівняно з міжнародними інституціями ситуація з національними іноземними неурядовими організаціями дещо гірша, адже рівень деталізації політик і застосування їх на практиці значною мірою залежить від віку організації, чутливості питань, з якими вона працює (так, робота з біженцями традиційно вважається більш чутливою, ніж надання допомоги на місцях, коли особи не піддаються переслідуванню чи не ризикують бути видворених з країни), а також розміру організації. Іншим варіантом, звісно ж, може бути відсутність політик у публічній площині, але це теж скоріше негативний показник, адже свідчить про неможливість отримувачів допомоги заздалегідь усвідомлювати, куди і як їхні дані можуть передаватися та для чого їх можуть використовувати. У будь-якому випадку, таку ситуацію варто змінювати.

Українські місцеві організації

Незалежно від виду та підстав надання гуманітарної допомоги, організації, що працюють з постраждалими або тими, хто потребує притулку, мають документувати і фіксувати порядок надання допомоги, а отже, збирати персональні дані. Українські організації не є винятком. Так, у Чернігові при видачі продуктових наборів реєстрували осіб, щоб продуктів вистачило всім, і збирали для цього мінімальну кількість інформації для ідентифікації особи. Така практика не є новою й для інших регіонів.

Водночас в Україні багато новостворених організацій — це природна реакція на повномасштабне вторгнення й суспільну потребу в гуманітарній допомозі, її організації та координації. Як зазначалося, з 24 лютого 2022 року кількість гуманітарних організацій зросла в п'ять разів порівняно з періодом до повномасштабного вторгнення. Новостворені організації часто орієнтувалися радше на надання самої допомоги, ніж на захист даних. І контекст, у якому вони діяли, явно не сприяв зміні акцентів чи обдумуванню другорядних речей. Тож з'ясуємо, чи змінилося щось із часом і чи, зрештою, українські організації мають адекватні політики захисту даних.

Українське товариство Червоного Хреста. Одна з найстаріших організацій, яка діє у сфері гуманітарних питань в Україні. Зауважимо, що національне товариство Червоного Хреста та МКЧХ — це не одна організація, вони мають різний порядок адміністрування. Наразі Товариство безпосередньо займається гуманітарною допомогою і має дуже високі показники в цій галузі. Національна організація має два види політик приватності — для донорів і для отримувачів допомоги. У цьому дослідженні варто зосередитися на другій.

> Повідомлення про обробку персональних даних розміщене на вебсайті організації та досить стисле Оскільки Товариство зареєстроване в Україні, більша частина Політики приватності містить посилання на національне законодавство:

- **види даних,** які збираються найчастіше (дані донорів, волонтерів, запитувачів інформації та підписників розсилки);
- **мета обробки даних** (ведення обліку донорів, відбір кандидатів для волонтерства, забезпечення відповідей на запити, відгуки чи скарги, інформування про діяльність Товариства);
- **застосовне регулювання** (українське законодавство);
- **права суб'єкта** (доступ до інформації, доступ до власних персональних даних, право запитувати видалення, зміну, знищення даних і заперечувати проти їх обробки, право відкликати згоду на обробку даних, захист від автоматизованих рішень);
- **передача даних** (співробітники, підрядники та волонтери, національні товариства Червоного Хреста або Червоного Півмісяця в інших країнах, МФЧХіЧП, оператори платіжних систем і фінансові установи, ділові партнери, агенти, професійні радники та постачальники послуг, поштові маркетингові сервіси);
- **файли кукіз** (з можливістю налаштувань);
- **строк зберігання** (стільки, скільки необхідно для досягнення мети обробки).

З політики помітно, що застосовна вона перш за все до інформації, яка збирається через вебсайт, тоді як жодної згадки про захист даних отримувачів допомоги політика приватності не містить. Окрім того, питання виникають щодо можливості передавати дані іншим національним товариствам, адже це потенційно передбачає можливість передачі даних у Росію. Водночас російське національне товариство порушує принцип нейтралітету й активно бере участь у збройному конфлікті, що наражає суб'єктів персональних даних на небезпеку. У випадку передачі даних цій організації інформація може потрапити до російського уряду і використовуватися для переслідувань українських громадян, які належать до вразливих груп.

У розділі вебсайту «Принципи та цінності» також відсутня згадка про персональні дані. Ані Статут, ані Стратегія Товариства на 2021–2025 роки не містять деталізації захисту даних отримувачів допомоги. Немає інформації про порядок роботи з персональними даними і в розділі «Часті запитання / відповіді», що свідчить про відносну неможливість для пересічного читача знайти інформацію про політики до того, як безпосередньо отримувати допомогу. Єдине, що дозволяє зрозуміти застосовні стандарти, — Постанова № 487 Кабінету Міністрів України про співпрацю з Червоним Хрестом, у якій зазначено, що до процесу роздачі гуманітарної допомоги застосовні вимоги Закону України «Про захист персональних даних».

Товариство наголосило, що проводить вибіркову верифікацію осіб, які подають заявки на компенсацію витрат розміщення ВПО. Це явно свідчить про обробку персональних даних організацією. Водночас деякі програми організації прямо зазначають відсутність вимог щодо збору та обробки персональних даних.

Відсутність кодифікованих політик чи щонайменше їх відсутність на вебсайті є негативним знаком, ще й тому, що Товариство є однією з провідних організацій у гуманітарній сфері. Це, власне, ставало підставами для інцидентів ще в часи COVID-19, коли Товариство було вимушене розвінчувати міфи про збір даних банківських карток. Також у березні 2023 року на вебсайт Товариства здійснили кібератаку, про що згодом повідомили користувачів. Утім, як зазначено в новині, персональні дані не постраждали.

Іншим тривожним дзвіночком стали численні спроби мімікрувати під працівників Товариства з метою крадіжки персональних даних. Наприклад, фейкові вуличні оголошення про надання гуманітарної допомоги. Також медіа повідомляли про створення фейкових Telegram-каналів Товариства для фішингу й крадіжки персональних даних підписників. Спроби шахрайства були зафіксовані, зокрема, на Тернопільщині. Це свідчить

про необхідність просвітницьких і комунікаційних кампаній щодо того, як справді виглядає допомога від національного товариства Червоного Хреста.

MacPaw Development Foundation. Благодійний фонд, заснований українською IT-компанією, який займається допомогою з 2016 року, а після повномасштабного вторгнення він переорієнтувався на допомогу постраждалим від російської агресії. Фонд має політику конфіденційності, яка застосовна до будь-яких даних, зібраних організацією.

Політика конфіденційності стосується вебсайту й даних, зібраних за його допомогою. Більша частина Політики приватності містить посилання на національне законодавство:

- **види даних,** які обробляють (контактні дані, технічні деталі, деталі використання вебсайту);
- **незастосовність до осіб, молодших за 13 років;**
- **застосовне регулювання** (українське законодавство та GDPR);
- **права суб'єкта** (доступ до інформації, право запитувати видалення, зміну, знищення даних і заперечувати проти їх обробки, право відкликати згоду на обробку даних);
- **передача даних** (лише органам правопорядку на правомірний запит);
- **файли кукіз** (з можливістю налаштувань);
- **витік даних** (обов'язок повідомляти).

На жаль, політиці бракує інформації про права користувачів надіслати запит щодо зміни чи видалення даних, а також можливість відкликати згоду на обробку даних.

Центр громадянських свобод (далі — ЦГС). Українська правозахисна організація, яка стала лауреатом Нобелівської премії миру й діє переважно в аналітичному напрямі на зразок вже аналізованої організації IMPACT. Аналізує персональні дані з метою прогнозування, підготовки аналітики чи проведення досліджень.

Політика конфіденційності стосується вебсайту й даних, зібраних за його допомогою. Більша частина політики приватності містить посилання на національне законодавство:

- **види даних**, які збираються найчастіше (заповнені форми, банківські перекази та кукіз);
- **мета обробки даних** (відбір кандидатів для волонтерства, забезпечення відповідей на запити, відгуки чи скарги, інформування про діяльність, публічні подяки);
- **застосовне регулювання** (українське законодавство);
- **передача даних** (лише органам правопорядку на правомірний запит);
- **файли кукіз** (з можливістю налаштувань).

На жаль, політиці бракує інформації про права користувачів надіслати запит щодо зміни чи видалення даних, а також можливість відкликати згоду на обробку даних. На противагу ЦГС, інші подібні громадські організації, як-от ZMINA, Платформа прав людини, Рух ЧЕСНО, які також працюють над створенням аналітичних продуктів та іноді можуть отримувати персональні дані отримувачів допомоги в дослідницьких цілях, не мають політик конфіденційності ані для роботи з такими питаннями, ані для власного вебсайту. Це досить прикра ситуація, особливо з огляду на те, що деякі із цих організацій напряму працюють з питаннями захисту даних.

Інші організації, які прямо чи опосередковано надають допомогу або є благодійниками, чия діяльність пов'язана зі збройним конфліктом, — БФ «Голоси дітей», Альянс громадського здоров'я, БФ «Клуб добродіїв», Право на захист, Карітас України, Рокада, Освітній дім прав людини в Чернігові, МБФ «Українська біржа благодійності», Проліска, Десяте квітня, — також не мають політик приватності навіть для вебсайту (тоді як політики приватності для роботи «в полі» або відсутні, або не оприлюднені). Деякі організації, як-от Волонтерська сотня Доброволя, узагалі діють переважно за допомогою мережі Facebook, де з політиками конфіденційності (та їх пошуком) ситуація ще складніша. Інші, на кшталт Stabilization Support Services, мають дуже розлогу систему політик, якій бракує лише політики із захисту даних. Прикро, що навіть організації, які працюють значно довше, ніж триває повномасштабне вторгнення, і вже тривалий час мають справу з гуманітарною допомогою, не мають політик, оприлюднених на власних вебсайтах, серед них КримSOS, ДонбасSOS і ВостокSOS.

Маємо і негативні випадки на місцевому рівні — у питаннях безпосереднього надання гуманітарної допомоги. Так, ГО «Броварська громада» стала фігурантом скандалу через надмірний збір персональних даних. Так, організація вимагала надання ІПН, а також даних про кількість членів родини та їхні контактні дані, що явно не пропорційно, наприклад, коли йдеться про одноразову фінансову допомогу. З приводу подібних випадків експерт **Олексій Кабанов** зазначає, що ці ситуації не поодинокі, скоріше це поширена практика для українських реалій. Експерт додає:

> ***«...гуманітарні організації, особливо дрібні, не мають затверджених порядків обробки персональних даних. ...Думаю, не складно в Facebook знайти повідомлення, які розповсюджуються мережею, з оприлюдненням надмірних даних про зниклих безвісти та їхніх родичів. Як правило, сім'ї таких осіб стають жертвами або ворожих добробажателів, або шахраїв. Оприлюднюють часто номери рідних, реквізити банківських рахунків, дані про зниклу особу (дата народження, чим любив займатись, хто друзі, де служив, що робив, фото з рідними і т. д.)».***

Інші організації, такі як Association Internationale de Cooperation Medicale, у відповідь на запит УМДПЛ прямо зазначили, що не поширюють жодну інформацію про роботу в Україні в цілях безпеки. З одного боку, позитивно, що організація взагалі відкрита для комунікацій, з іншого, це не допомагає отримувачам допомоги зрозуміти, наскільки вони будуть у безпеці, якщо звернуться до такої благодійної організації.

Також є низка державних і напівдержавних програм, орієнтованих на полегшення доступу до гуманітарної допомоги. До них належать ЄДопомога та СпівДія. Обидві ініціативи мають досить розлого прописані політики, які можна знайти за відповідними посиланнями (перша і друга). На жаль, Політика ЄДопомоги досить мало уваги приділяє саме захисту персональних даних, а тому більшість традиційних прав суб'єктів при реєстрації для отримання допомоги цим документом фактично не передбачені. І це теж проблема, адже державні ініціативи часто сприймаються приватними організаціями як еталон. Коли ж у державних ініціатив бракує відповідального ставлення до формулювання політик приватності, приватний сектор може сприймати це як «зелене світло» для подібного ставлення.

Короткі висновки можна вважати скоріше невтішними: більшість національних гуманітарних організацій щонайменше не мають політик захисту даних на власних вебсайтах. Отже, громадяни, які потребують допомоги, не здатні належним чином ознайомитися з власними правами, передбачити, куди і як можуть передаватися дані. З цього приводу експертка у сфері захисту персональних даних **Тетяна Олексіюк** прямо зазначила, що громадський сектор рідко ознайомлює отримувачів допомоги з політиками приватності. Також вона наголосила:

> ***«...не слід очікувати, що отримувачі гуманітарної допомоги (а це люди, які опинилися у скрутних життєвих обставинах і є вразливими), будуть почуватися достатньо впевненими, щоб наполягати на дотриманні вимог щодо захисту***

їхніх персональних даних. Для людей, які опинилися на межі виживання, це не видається пріоритетом».

Експерт із цифрових прав **Віталій Мороз** також додає з досвіду взаємодії з громадським сектором, що організації, на жаль, дуже рідко мають детальні політики захисту даних, адже це вимагає обізнаності в темі захисту даних, постійного юридичного супроводу цього питання й бажання пріоритезувати цей напрям у діяльності організації. На думку експерта, часто гуманітарні організації навіть не мають політик приватності на вебсайтах, не кажучи вже про окремі політики захисту даних для надання допомоги.

Тож, на превеликий жаль, культура захисту персональних даних в Україні є не надто високою, утім, правозахисні організації саме ті актори, які мають брати до уваги небезпеки, пов'язані з витоками даних і хакерськими атаками. Особливо ті організації, які зареєстровані та діють в Україні, а тому природно перебувають у зоні підвищеного ризику через російську агресію.

РОЗДІЛ V.
Рекомендації

Захист персональних даних під час збройного конфлікту — завдання не лише гуманітарних організацій, до цього процесу має долучатися кожен стейкхолдер. Зокрема, тому, що політики організацій часто залежать від національного регулювання, а практика роботи із захистом персональних даних — від обізнаності отримувачів допомоги про свої права, готовність інших правозахисних організацій стежити за дотриманням стандартів, а також рівня технічної та правової експертизи наглядових органів. Саме тому до захисту персональних даних під час надання гуманітарної допомоги неодмінно слід підходити комплексно. Аналіз міжнародних і національних стандартів, політик і практик гуманітарних організацій дозволив напрацювати низку рекомендацій, представлених нижче.

Для національних урядів:

- Розробити чітке національне законодавство, яке адекватно регулюватиме питання збору й обробки персональних даних, у тому числі в гуманітарних цілях (наприклад, передбачити застосовність Закону України «Про захист персональних даних» до діяльності, пов'язаної з наданням гуманітарної допомоги, у профільному законі).

- Оновити застаріле законодавство про захист персональних даних у разі, якщо воно не відповідає чинним міжнародним стандартам, не передбачає рамкових обмежень на використання автоматизованих технологій чи запобіжників від зловживань ними (як-от автоматизоване ухвалення рішень, системи, керовані штучним інтелектом тощо).

- Забезпечити можливість легкої та швидкої комунікації гуманітарних організацій з державними органами, відповідальними за захист даних, уможливити роз'яснення національних стандартів іноземним організаціям.

- Комунікувати з донорськими установами для послаблення вимог щодо передачі великих масивів персональних даних від гуманітарних організацій-реципієнтів як звітної інформації. Роз'яснювати чутливість контекстів, у яких оперують гуманітарні організації.

- Комунікувати злами державних баз даних і витоки даних, щоб гуманітарні організації мали уявлення про безпекову ситуацію з персональними даними в регіоні та безпосередньо в державах, де вони зареєстровані чи надають допомогу.

Для гуманітарних організацій:

- Розробити політики захисту даних у випадках, якщо такі політики відсутні. Оновити застарілі чи нерелевантні політики, адаптувати їх до контексту роботи гуманітарної організації та технологій, які вона використовує при зборі й обробці даних.

- Розміщувати політики на видному місці на вебсайті організації, забезпечувати легкий доступ потенційних отримувачів допомоги до політик, вчасно повідомляти про їх оновлення.

- Зазначати в політиці, що вона застосовна до всіх видів обробки даних, які здійснює організація, або якщо політика застосовна лише до збору даних через вебсайт, чітко згадувати про це в назві політики й давати посилання на політику, яка застосовна до інших зборів даних, зокрема процесів надання гуманітарної допомоги.

- Формулювати політики зрозумілою мовою, робити їх стислими й лаконічними (наприклад, Політика Світової продовольчої програми ООН на 130 сторінок явно не сприяє ознайомленню з нею пересічних отримувачів допомоги в критичних ситуаціях).

- Розробити версію політики, сформульовану доступною для дітей мовою, у разі, якщо фокусом організації є робота з дітьми та надання їм гуманітарної допомоги.

- Чітко і вичерпно описувати в політиці перелік даних, які збираються, і мету збору конкретних категорій даних (зокрема, це допоможе самим гуманітарним організаціям з'ясувати, чи вони не збирають дані в надмірних кількостях і чи є кількість даних пропорційною меті).

- Регулярно проводити оцінювання ризиків діяльності для захисту персональних даних, переглядати політики захисту даних залежно від контексту роботи, виду надаваної гуманітарної допомоги та засобів обробки даних, які використовуються організацією:

  - оцінювання має проводитися до, під час та після надання гуманітарної допомоги
  - оцінювання має ґрунтуватися на рівні ризиків від певної активності, застосування певної технології чи певних дій у конкретному контексті;
  - оцінювання має орієнтуватися на підхід «приватність за замовчуванням»;
  - оцінювання має враховувати технологічний розвиток суспільства й ефективність технологій для подолання конкретних викликів;
  - оцінювання має мати прикладне, а не формальне значення.

- Уникати надміру широких підстав для збору і обробки даних при формулюванні політик захисту персональних даних, зокрема не включати «суспільний інтерес» чи «легітимний інтерес організації» до підстав обробки даних без належної деталізації.

- Мінімізувати збір даних, особливо у випадках, якщо організація є невеликою за кількістю персоналу й експертизою або нездатною повноцінно забезпечити безпеку даних з технічної та правової точки зору. Це особливо актуально тоді, коли організація планує збирати біометричні дані чи працює з технологіями, що потребують значного залучення технічних експертів.

- Надавати біженцям і шукачам притулку доступ до даних про них, пояснювати мету збору та порядок обробки даних, подальшу долю цієї інформації. У разі помилки в даних надавати можливість виправити інформацію.

- При використанні сторонніх ресурсів (програмного забезпечення, додатків чи вебсайтів, як-от «Trace the Face» у МКЧХ) для ідентифікації осіб, створення баз даних чи в інших цілях, пов'язаних з наданням гуманітарної допомоги, розміщувати політику захисту даних на таких ресурсах, викладати її зрозуміло й стисло, де можливо – додавати мови регіону, з яким гуманітарна організація активно працює.

- Утримуватися від поширення даних з державою чи іншими акторами, особливо коли це відбувається без попередження осіб, чиї дані планується передавати. У разі, якщо йдеться про вразливі групи, які можуть бути дискриміновані в державі, у якій надається гуманітарна допомога, дотримуватися максимальної конфіденційності в комунікаціях з державним сектором.

- Ретельно зважувати ризики при передачі систем прогнозування хвиль мігрантів, біженців та інших осіб, які потребують гуманітарної допомоги, державі (зокрема, як це сталося із системою, розробленою Danish Refugee Council). Це особливо важливо в контексті роботи в недемократичних режимах, де держава може спробувати обміняти дозвіл на роботу в регіоні на доступ до технологій.

- Призначити особу, відповідальну за захист даних, і розмістити контакти такої особи на вебсайті, щоб уможливити комунікацію будь-яких зацікавлених сторін з експертом із захисту даних усередині гуманітарної організації.

- Чітко вказувати підстави збору біометричних даних і те, наскільки це допомагає уникнути шахрайств, поліпшити процеси ідентифікації та знизити витрати на надання

гуманітарної допомоги (включно з фінансовими й технічними розрахунками та показниками ефективності для доступних альтернатив збору персональних даних).

- Посилювати навички роботи з персональними даними в правовій і технічній площині для персоналу гуманітарної організації, який безпосередньо чи опосередковано працює з даними. Зокрема, у пригоді можуть стати освітні програми і сертифікації від МКЧХ та академічних закладів.

- Використовувати додатки з адміністрування паролів для посиленого захисту, що може убезпечити від використання викрадених персональних даних чи зламаних акаунтів для неправомірних активностей.

- Для уникнення витоків даних і зламів системи встановити програми застосування оновлень безпеки, регулярно проходити аудити для оцінювання вразливості систем (тестувати нові системи й перевіряти спроможність старих протистояти новим викликам і загрозам).

- Розробляти кризові протоколи на випадок зламів чи атак, які міститимуть чіткий алгоритм дій членів організації, залучених до роботи з персональними даними, регулярно переглядати та оновлювати такі протоколи залежно від контексту діяльності та застосовних технологій обробки даних.

- У випадку кібератаки чи витоку даних слід вчасно комунікувати з тими, чиї дані можуть опинитися чи опинилися під загрозою про наявну загрозу, проаналізувати прогалини в системі безпеки та оновити / посилити / змінити політики в разі потреби.

- Не використовувати для збору даних мережі на кшталт Telegram, Facebook чи інших незахищених соціальних мереж і месенджерів. Використовувати канали комунікації, які містять з'єднання peer-to-peer і можливість видаляти переписки із сервера для забезпечення максимальної конфіденційності.

Для донорських організацій:

- Включити захист даних у планування проєктів і звітних форм, враховуючи чутливі контексти, у яких зазвичай оперують організації, що реалізують гуманітарні проєкти.

- Дотримуватися принципу мінімізації даних та утримуватися від вимагання надмірної кількості чутливої інформації (зокрема, не вимагати інформацію про стать, сексуальну орієнтацію, походження, належність отримувачів допомоги до маргіналізованих чи вразливих груп тощо).

- Бути гнучкими й адаптивними, коли безпосередній надавач допомоги зазначає про особливу чутливість отриманих даних і відмовляється включати таку інформацію до звітних форм.

- Переглянути технічні стандарти передачі даних від гуманітарної до донорської організації та посилити захист даних у разі, якщо виникають сумніви в надійності каналів комунікації. Якщо це неможливо, відмовитися від передачі особливо чутливих категорій даних.

Для отримувачів гуманітарної допомоги:

- Користуватися ініціативами захисту прав українців від правозахисних організацій, інформаційними ресурсами та керівництвами з отримання допомоги (на кшталт сторінки «Солідарність ЄС з Україною»).

- Обережно ставитися до надання персональних даних для отримання гуманітарної

допомоги чи участі в так званих переписах населення на окупованих територіях, не розкривати інформації про військовослужбовців, членів їхніх сімей, громадських активістів, журналістів, культурних діячів.

- Уникати сайтів чи цифрових застосунків, у безпечності яких немає впевненості. Щонайменше не використовувати такі застосунки для передачі персональних даних.

- Уважно ставитися до електронних листів від незнайомих адресатів, повідомлень у месенджерах (Viber, Telegram, WhatsApp) з невідомих номерів телефону, а також повідомлень у соціальних мережах (Facebook, Instagram) від незнайомих користувачів, не відкривати підозрілі посилання та файли.

- За можливості при авторизації в інформаційних системах, сайтах, електронних кабінетах використовувати дво- або багатофакторну аутентифікацію та дотримуватися інших правил цифрової безпеки. З ними можна ознайомитися на ресурсі «Як?».

- Обережно ставитися до сканування QR-кодів для виконання будь-яких дій, пов'язаних з наданням персональних даних, отриманням допомоги чи інформації про надання допомоги, адже QR-код може вести до неперевірених посилань і, як наслідок, завантаження шкідливого програмного забезпечення q крадіжки даних з девайсу.

- Відмовитися від передачі персональних даних, включаючи паролі доступу до акаунтів, разові паролі, дані геолокації тощо, третім особам до моменту виникнення законних і необхідних підстав для збору такої інформації.

- Не надавати свої персональні дані та згоду на їхню обробку до моменту ознайомлення з метою та підставами обробки персональних даних, а також умовами їх обробки (зокрема, ознайомлення з політиками конфіденційності), окрім випадків, коли відповідна обробка здійснюється на підставі закону для виконання володільцем даних покладених на нього обов'язків.

- Направляти запити щодо інформації про джерела збирання, місцезнаходження своїх персональних даних, мету їх обробки, місцезнаходження володільця чи розпорядника персональних даних.

- Висувати вмотивовану вимогу володільцю персональних даних із запереченням проти обробки своїх персональних даних, зміни або знищення своїх персональних даних, якщо ці дані обробляються незаконно чи є неправильними.

- Відкликати згоду на обробку персональних даних (у випадку, якщо згоду було надано).

- Використовувати для отримання інформації надійні джерела, наприклад моніторинг IMI надає перелік добросовісних медіа, які дотримуються журналістських стандартів.

- Брати участь у розробленні політик захисту даних на рівні держави, гуманітарних і донорських організацій, ділитися досвідом щодо проблем, які виникли на практиці під час отримання гуманітарної допомоги, пропонувати рішення для посилення захисту даних, покращення політик конфіденційності тощо.

Для правозахисних організацій:

- Сприяти підвищенню рівня обізнаності гуманітарних організацій щодо правил роботи з персональними даними, оскільки не всі гуманітарні організації є правозахисними і тому можуть мати брак як правової, так і технічної експертизи.

- Ділитися позитивними практиками захисту даних (у тому числі формулюваннями політик), безпечного збору даних і їх передачі третім особам (за потреби), повідомляти

про негативні досвіди для уникнення подібних ситуацій у роботі інших організацій.

- Засуджувати випадки порушення правил роботи з персональними даними, нехтувань технічною безпекою, зловживань чи маніпуляцій отримувачами допомоги завдяки більш привілейованому становищу гуманітарної організації (розпорядника ресурсів).

- Комунікувати проблемні випадки захисту даних і потенційні шляхи розв'язання проблем державі (регуляторні політики та звітування), донорським організаціям (звіти q обсяги даних), гуманітарним організаціям (потенційна зміна практики), громадянам (підвищення рівня цифрової грамотності, уміння захищати власні персональні дані).

Для медіа:

- Утримуватися від поширення неперевірених даних про порушення гуманітарними організаціями правил поводження з даними, оскільки неправдива інформація здатна підірвати довіру до гуманітарного сектору, спричиняючи неотримання допомоги тими, хто її потребує.

- Контактувати з організаціями, у яких, ймовірно, відбувся витік даних чи бази даних яких могли стати суб'єктом хакерської атаки, з метою верифікації інформації та отримання широкого погляду на проблему.

- Утримуватися від перебільшення наслідків витоків даних або кібератак (наприклад, DoS-атака не дорівнює зламу бази даних, відповідно шкода для персональних даних буде значно меншою, якщо не нульовою, тож їх не слід ототожнювати).

- У разі витоку даних у мережу утриматися від подальшого поширення персональних даних і збільшення аудиторії, яка має доступ до чутливої інформації.

- Популяризувати кампанії, спрямовані на підвищення обізнаності про правила захисту даних серед громадян і програми розвитку здатності гуманітарних організацій забезпечувати захист персональних даних (тренінги від держави, інших громадських організацій, академічної спільноти тощо).