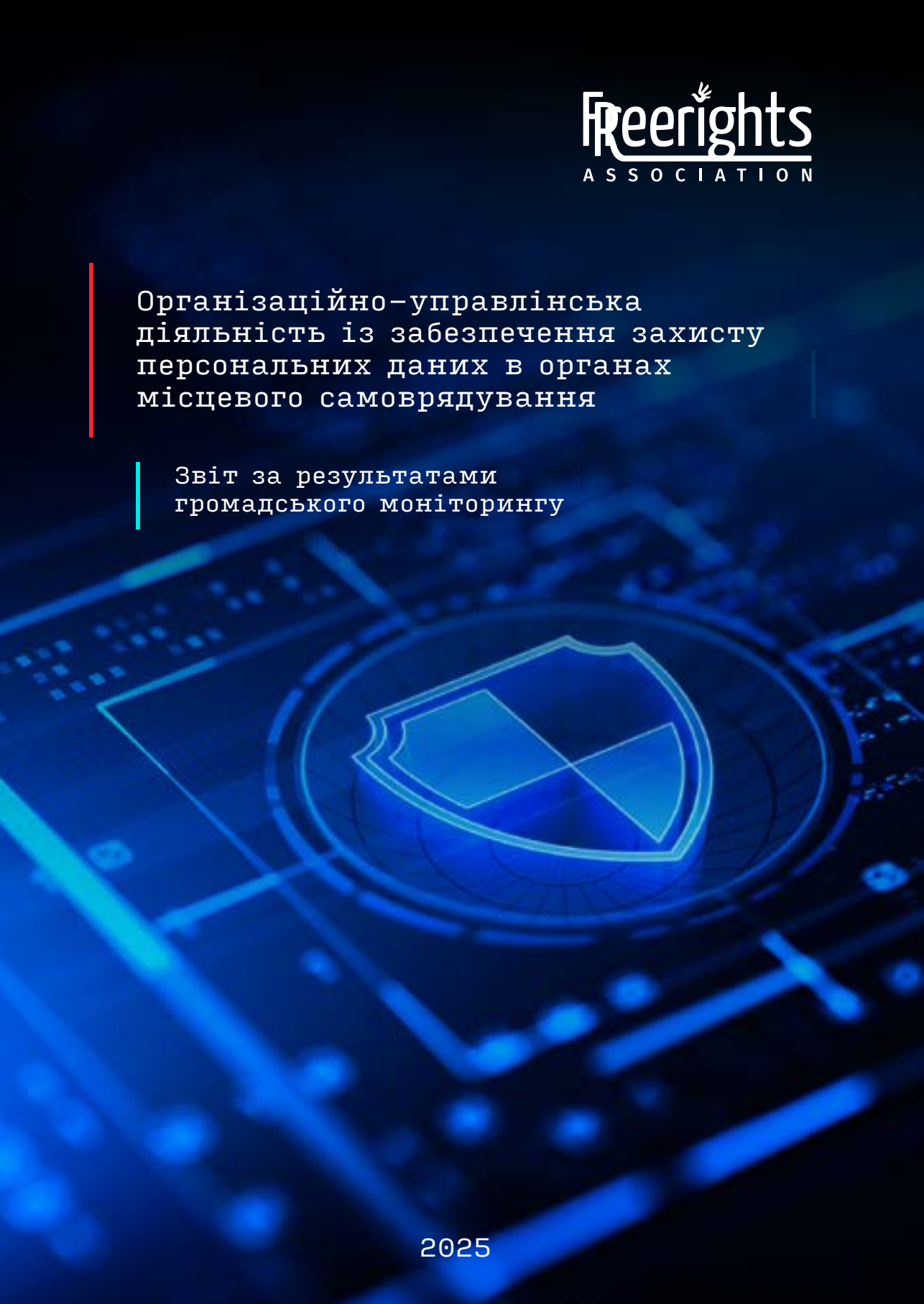
Freerights
ASSOCIATION

Організаційно-управлінська діяльність із забезпечення захисту персональних даних в органах місцевого самоврядування

Звіт за результатами громадського моніторингу



2025

Організаційно-управлінська діяльність із забезпечення захисту персональних даних в органах місцевого самоврядування (звіт за результатами громадського моніторингу) — Київ: Асоціація Freerights, 2025 — 28 с.

Матеріал підготовлено за підтримки Міжнародного фонду «Відродження». Погляди авторів Звіту за результатами громадського моніторингу «Організаційно-управлінська діяльність із забезпечення захисту персональних даних в органах місцевого самоврядування» не обов'язково відображають позицію Міжнародного фонду «Відродження».

Зміст

1. Актуальність проблеми

З початку повномасштабного вторгнення російської армії в Україну експерти Асоціації *Freerights* відстежують та досліджують ситуацію із захистом персональних даних в країні. На жаль, всебічний аналіз стану справ у цій сфері не дає підстав для позитивних висновків і оптимістичних прогнозів. Публікації в онлайн-медіа і соціальних мережах, інша отримана з відкритих джерел інформація свідчить: недооцінка загроз безпеці персональних даних не тільки завдала шкоди національним і військовим інтересам України, а й призвела до людських втрат.

Було б неправильним пояснювати проблему лише недосконалістю законодавства або зводити її виключно до пасивності влади у створенні комплексної та багаторівневої системи захисту персональних даних в державі. Дієвість такої системи загалом залежить від ефективності функціонування кожного її компонента, зокрема й органів місцевого самоврядування, де досягнути суттєвого покращення рівня захисту персональних даних цілком можливо у межах існуючого правового регулювання та за відсутності додаткових директив з боку уряду. В міських, селищних та сільських радах провідного значення набуває людський фактор, коли компетентність, сумлінність й доброчесність працівників, задіяних у процесах обробки й захисту інформації, відіграють не меншу роль, ніж технічні засоби і прогресивні юридичні акти.

Саме тому правозахисники та експерти давно й наполегливо намагаються привернути увагу очільників органів місцевого самоврядування до недоліків і прорахунків, яких можна й необхідно уникати. Зокрема:

- збирання та накопичення надлишкових персональних даних, непотрібних для досягнення офіційно задекларованих цілей їх обробки;
- формальне ставлення до запровадження заходів безпеки при обробці персональних даних, порушення умов і строків їх зберігання, а також порядку доступу до них;
- відсутність цілеспрямованого внутрішнього контролю з боку керівництва за станом захищеності персональних даних;
- неефективність розслідувань інцидентів безпеки та випадків порушень обробки персональних даних;
- незадовільна підготовка персоналу щодо нормативно-правових засад захисту персональних даних;
- невідповідність використовуваних засобів захисту інформації вимогам сьогодення та можливостям передових технологій.

Окупація частини країни наочно підтвердила обґрунтованість пересторог правозахисників — жахливою ціною за ці прорахунки стали втрачені

життя, здоров'я і свобода багатьох людей, які опинились на захоплених ворогом територіях.

Для відстеження тенденцій та динаміки змін у ставленні до захисту персональних даних в органах місцевого самоврядування після трьох років повномасштабної війни, в січні-травні 2025 року Асоціація *Freerights* провела моніторингову кампанію із залученням до збору інформації регіональних координаторів Уповноваженого ВРУ з прав людини[1] та подальшим опрацюванням отриманих даних експертами Асоціації.

2. Моніторингова кампанія

До моніторингової кампанії були залучені регіональні координатори з **12 областей України,** які здійснили моніторинг **50 органів місцевого самоврядування** (19 міських, 18 селищних та 13 сільських рад). Об'єктом моніторингу стала організаційно-управлінська діяльність із забезпечення дотримання вимог законодавства про захист персональних даних.

Відповідно до визначених цілей, експертами Асоціації *Freerights* був розроблений інструментарій для здійснення моніторингу: уніфікована анкета (чекліст) з критеріями оцінювання роботи органу місцевого самоврядування із захисту персональних даних та зразок стандартного запиту на отримання відповідної публічної інформації. Також експертами Асоціації підготовлені рекомендації щодо порядку проведення моніторингової кампанії та організовано 7 спеціалізованих семінарів, на яких регіональні координатори отримали знання, необхідні для виконання завдань моніторингу з високим рівнем компетентності.

Цілі моніторингу:

— отримання, узагальнення та аналіз інформації про стан управлінської діяльності з організації захисту персональних даних в міських, селищних, сільських радах. Визначення типових недоліків і прорахунків у такій роботі;

— сприяння усвідомленню посадовими особами органів місцевого самоврядування важливості питань захисту персональних даних та налагодження співпраці з громадськістю у цій сфері;

1 Надалі у тексті — регіональні координатори

— набуття регіональними координаторами досвіду й навичок використання моніторингу як засобу громадського контролю за дотриманням прав громадян в міських, селищних, сільських радах.

Аспекти діяльності органів місцевого самоврядування, що вивчалися під час моніторингу:

— стан дотримання законодавства України про захист персональних даних, зокрема виконання вимог до ведення внутрішньої службової документації та взаємодії з Уповноваженим ВРУ з прав людини;

— порядок здійснення внутрішнього контролю за процесами обробки та захисту персональних даних;

— організація навчання персоналу, залученого до роботи з персональними даними;

— проведення інформаційно-просвітницьких заходів у місцевих громадах щодо прав громадян, як суб'єктів персональних даних;

— забезпечення захисту персональних даних, отриманих з використанням систем відеоспостереження та офіційного вебсайту.

Моніторинг здійснювався з використанням наступних методів:

— опитування або анкетування посадових осіб міських, селищних та сільських рад, зокрема відповідальних за роботу з персональними даними;

— надсилання до органів місцевого самоврядування запитів на отримання публічної інформації;

— відвідування службових приміщень міських, селищних, сільських рад з вільним режимом доступу;

— аналіз матеріалів, опублікованих на вебсайтах органів місцевого самоврядування.

Проведення моніторингу не передбачало безпосереднього доступу до персональних даних громадян, не порушувало вимог режиму секретності та жодним чином не заважало працівникам міських, селищних, сільських рад виконувати свої службові обов'язки.

3. Результати моніторингу

3.1. Ведення службової документації

Управлінська діяльність в органі місцевого самоврядування неможлива без створення та підтримання в актуальному стані значної кількості власних розпорядчих документів, якість підготовки яких впливає на ефективність роботи органу. Така документація посідає важливе місце і в забезпеченні захисту персональних даних, оскільки саме внутрішні документи з одного боку роз'яснюють, уточнюють та деталізують відповідні норми законодавства, з іншого — описують способи їх виконання та визначають необхідні для цього сили й засоби.

Закон України *«Про захист персональних даних»* не містить переліку конкретних документів, які необхідно розробити володільцю/розпоряднику персональних даних, але зобов'язує його до виконання низки важливих заходів і процедур, хід здійснення та кінцеві результати яких мають бути зафіксовані в електронному або паперовому вигляді. Зокрема, володілець/розпорядник повинен визначити мету роботи з персональними даними, порядок їх обробки, забезпечення цілісності, поширення, видалення або знищення, регламентувати доступ до персональних даних третіх осіб, організувати повідомлення суб'єкта персональних даних про його права, письмово інформувати про свою роботу Уповноваженого ВРУ з прав людини, проводити навчання працівників, які залучені до обробки персональних даних, тощо. Зрозуміло, що реалізація цих завдань потребує створення окремого пакету внутрішніх організаційних, технологічних та методичних документів.

З огляду на це, Офісом Омбудсмана України були розроблені регуляторні акти, а також рекомендації та роз'яснення з питань ведення документації щодо з*ахисту персональних даних, у тому числі:*

- *«Типовий порядок обробки персональних даних»;*
- *«Порядок здійснення Уповноваженим ВРУ з прав людини контролю за додержанням законодавства про захист персональних даних»;*
- *«Порядок повідомлення Уповноваженого ВРУ з прав людини про обробку персональних даних, яка становить ризик для прав і свобод суб'єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних при їх обробці, а також оприлюднення вказаної інформації»;*
- *«Роз'яснення до Типового порядку обробки персональних даних»;*

— *«Роз'яснення до Порядку здійснення Уповноваженим контролю за додержанням законодавства про захист персональних даних»;*

— *«Роз'яснення до основних положень Порядку повідомлення Уповноваженого щодо визначення обробки персональних даних, яка становить ризик для прав і свобод суб'єктів персональних даних»;*

— *«Лист Уповноваженого Верховної Ради України з прав людини № 2/9-227067.14-1/НД-129 від 03.03.2014 щодо захисту персональних даних»;*

— *«Рекомендації Уповноваженого Верховної Ради України з прав людини щодо дотримання права на приватність під час встановлення і використання систем відеоспостереження у громадських місцях».*

Проте формування цієї нормативної бази не спонукало органи місцевого самоврядування до проведення аналогічної роботи на місцевому рівні. Моніторинг показав, що наразі в міських, селищних, сільських радах не приділяють належної уваги підготовці власних розпорядчих документів з управління процесами обробки персональних даних, що негативно впливає на рівень їх захищеності.

Згідно з пунктом 1 *«Типового порядку обробки персональних даних»,* їх власник повинен самостійно встановити порядок такої обробки з урахуванням сфери та специфіки своєї діяльності. Пункт 2 цього Порядку вказує, які саме напрямки роботи з персональними даними мають бути регламентовані. Зокрема, у спеціальному документі необхідно визначити склад персональних даних, мету та підстави їх обробки, умови поширення та передачі третім особам, заходи із захисту персональних даних, гарантії дотримання прав громадян та інше. Зазвичай таким документом є ***«Політика (положення) щодо обробки персональних даних»,*** яку можна вважати правовим фундаментом роботи з персональними даними в органі місцевого самоврядування. Проте ***у 62%***[2] міських, селищних, сільських рад *«Політика щодо обробки персональних даних»* або інший подібний документ відсутні.

Подібна ситуація спостерігається і зі створенням ***«Реєстру обробки персональних даних»,*** в якому мають фіксуватися всі операції, пов'язані з обробкою персональних даних та доступом до них. Реєстр надає можливість відстежувати та контролювати обіг персональних даних на всіх етапах роботи з ними — від отримання й архівування до поширення й знищення. Попри те, що необхідність зберігання такої інформації передбачається підпунктами 2.1., 3.4., 3.11. *«Типового порядку обробки персональних даних»*, у **80%** міських, селищних, сільських рад *«Реєстр обробки персональних даних»* не ведеться.

Підпункт 3.4. *«Типового порядку обробки персональних даних»* вказує на необхідність підготовки володільцем/розпорядником ***«Плану дій на***

2 Тут і надалі вказується відсоток від загальної кількості охоплених моніторингом органів місцевого самоврядування

випадок несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, виникнення надзвичайних ситуацій», але **74%** органів місцевого самоврядування подібного плану не мають, а отже за необхідності швидко відреагувати на кризові події не зможуть.

Одним з важливих організаційних заходів із запобігання витоку персональних даних є **контроль за їх своєчасним видаленням або знищенням.** Відповідно до статті 6 Закону України *«Про захист персональних даних»*, дані повинні зберігатися не довше, ніж це необхідно для досягнення законних цілей їх обробки. Підпункти 2.1., 3.11. *«Типового порядку обробки персональних даних»* вимагають від володільця/розпорядника персональних даних не тільки визначити строки та умови їх зберігання, а й обліковувати та зберігати відомості про мету, підстави, дату видалення (знищення) персональних даних і працівників, які здійснювали такі операції. Результати моніторингу свідчать, що всупереч цим вимогам у **76%** міських, селищних, сільських рад відсутній документ, що встановлює строки та умови зберігання персональних даних різних категорій. Також у **76%** органів місцевого самоврядування не регламентована процедура знищення (видалення) персональних даних після закінчення строку їх зберігання, а факти проведення такого знищення (видалення) не фіксуються документально складанням акта, записами у журналі чи внесенням відповідних даних до реєстру.

В більшості відвіданих рад виявлені недоліки у нормативному врегулюванні взаємин між суб'єктами правовідносин, пов'язаних з персональними даними. У **86%** міських, селищних, сільських рад не розроблений документ, що визначає **перелік третіх осіб, яким можуть бути передані персональні дані,** та умови й процедуру здійснення такої передачі, хоча наявність цього документа передбачена підпунктом 2.1. *«Типового порядку обробки персональних даних»*. Попри те, що підпункти 2.1., 3.5. Порядку зобов'язують володільця/розпорядника вести **облік працівників, які мають доступ до персональних даних** та встановити рівень і порядок такого доступу, у **80%** органів місцевого самоврядування цей облік відсутній, а у **70%** — не має **посадових інструкції для працівників,** залучених до обробки персональних даних.

Стаття 12 Закону України *«Про захист персональних даних»* наголошує на необхідності повідомлення суб'єкта персональних даних про його права, визначені цим Законом. Підпункт 2.9 *«Типового порядку обробки персональних даних»* доповнює цю вимогу та покладає на володільця персональних даних обов'язок зберігати інформацію (документи), які підтверджують факт такого повідомлення, протягом усього періоду обробки персональних даних. Моніторинг показав, що у **48%** міських, селищних, сільських рад суб'єкти персональних даних взагалі не ознайомлюються зі своїми правами. Варто зауважити, що нормативні акти не описують процедуру повідомлення суб'єкта персональних даних про його права та не визначають

форму документа, який би засвідчував її проведення. Така невизначеність призвела до того, що, як правило, в органах місцевого самоврядування з правами суб'єкта персональних даних ознайомлюються лише працівники при прийнятті на роботу. Відвідувачі інформуються про ці права лише у **22%** міських, селищних, сільських рад, при цьому ознайомлення з правами часто здійснюється без документального підтвердження — за словами посадових осіб *«про права повідомляємо усно», «громадяни вважаються ознайомленими з правами, оскільки на інформаційному стенді у вестибюлі є витяг Закону України «Про захист персональних даних».*

Подібне ставлення спостерігається і до виконання вимог статті 10 Закону України *«Про захист персональних даних»* та підпункту 3.7. *«Типового порядку обробки персональних даних»*, якими передбачається отримання від працівників письмових ***«Зобов'язань про нерозголошення персональних даних»***, довірених їм у зв'язку з виконанням службових обов'язків. У **54%** міських, селищних та сільських рад відбирання таких зобов'язань не практикується.

3.2. Відповідальні особи та взаємодія з Уповноваженим ВРУ з прав людини

На думку експертів Асоціації Freerights, однією з причин недостатньої захищеності персональних даних в органах місцевого самоврядування є відсутність кваліфікованого менеджменту у цій сфері. Стаття 24 Закону України *«Про захист персональних даних»* вказує: *«В органах державної влади, органах місцевого самоврядування, а також у володільцях чи розпорядниках персональних даних, що здійснюють обробку персональних даних, яка підлягає повідомленню відповідно до цього Закону, створюється (визначається) структурний підрозділ або* ***відповідальна особа, що організовує роботу, пов'язану із захистом персональних даних при їх обробці****»*. Попри це, у **74%** міських, селищних, сільських рад такі відповідальні особи чи структурні підрозділи наразі відсутні.

Слід зазначити, що стаття окремо акцентує увагу на необхідності призначення відповідальної особи у випадку, коли володілець/розпорядник займається обробкою персональних даних, *«яка підлягає повідомленню»*, тобто працює з персональними даними, обробка яких становить особливий ризик для прав і свобод громадян.[3] Проте у **71%** міських, селищних, сільських рад, де підтвердили факт обробки таких даних, цю вимогу також не виконали і відповідальну особу не призначили.

3 Надалі у тексті — вразливі персональні дані

Результати моніторингу свідчать, що в органах місцевого самоврядування призначення відповідальної особи часто має суто номінальний характер і є скоріше даниною вимогам законодавства, ніж піклуванням про інформаційну безпеку. На це вказує той факт, що у **38%** міських, селищних, сільських рад, де відповідальні особи були призначені, не розроблений документ, який би визначав їх права та обов'язки, хоча наявність такого документа передбачає підпункт 2.2. *«Типового порядку обробки персональних даних»*.

Нормативно-правові акти описують функції та завдання відповідальної особи лише у загальних рисах, без конкретизації способів та інструментів їх виконання. Така ситуація вимагає від призначених на цю ділянку роботи посадовців ініціативності, прагнення до самовдосконалення, здатності самостійно приймати рішення та готовності брати на себе відповідальність за їх реалізацію. Поки що відповідальним особам у міських, селищних, сільських радах ці ділові якості не притаманні, про що свідчать практичні результати їх роботи, а точніше — відсутність таких результатів.

Зокрема на це вказує незадовільний **рівень взаємодії органів місцевого самоврядування з Офісом Омбудсмана України.** Відповідно до статті 24 Закону України *«Про захист персональних даних»*, інформацію про призначення відповідальної особи необхідно направляти Уповноваженому Верховної Ради України з прав людини, який забезпечує її оприлюднення. Попри те, що форма такого повідомлення та процедура його направлення затверджені наказом Уповноваженого від 08.01.2014 №1/02-14, **77%** міських, селищних, сільських рад, де відповідальна особа була призначена, **Офіс Омбудсмана про це не проінформували.**

Згідно з вимогами статті 9 Закону України *«Про захист персональних даних»*, органи місцевого самоврядування, які працюють з вразливими персональними даними, також повинні письмово повідомляти про це Секретаріат Уповноваженого ВРУ з прав людини. Під час моніторингу з'ясовано, що **83%** міських, селищних, сільських рад, де підтвердили здійснення обробки вразливих даних, відповідну інформацію до Офісу Омбудсмана не направили.

У **21** органі місцевого самоврядування посадові особи заявили, що обробка вразливих персональних даних ними не здійснюється, а отже в інформуванні Уповноваженого потреби немає. Подібні твердження викликали у експертів обґрунтовані сумніви.

Відповідно до підпункту 1.2. *«Порядку повідомлення Уповноваженого ВР України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних при їх обробці, а також оприлюднення вказаної*

інформації» (затверджений наказом Уповноваженого ВРУ з прав людини від 08.01.2014 №1/02-14), до категорії вразливих відносяться персональні дані про:

- расове, етнічне та національне походження, політичні, релігійні або світоглядні переконання;
- членство в політичних партіях та/або організаціях, професійних спілках, релігійних організаціях чи в громадських організаціях світоглядної спрямованості;
- стан здоров'я та статеве життя, а також біометричні та генетичні дані;
- **притягнення до адміністративної чи кримінальної відповідальності,** а також застосування щодо особи заходів в рамках досудового розслідування;
- вжиття щодо особи заходів, передбачених Законом України «Про оперативно-розшукову діяльність»;
- вчинення щодо особи тих чи інших видів насильства;
- місцеперебування та/або шляхи пересування особи.

Аналіз зазначеного переліку у контексті стандартних напрямків діяльності органів місцевого самоврядування дає підстави вважати, що у більшості міських, селищних, сільських рад у той чи інший спосіб здійснюється обробка певних видів вразливих персональних даних, а посадовці, які заявляють про протилежне, просто не знають, які саме дані належать до цієї категорії. Такий висновок підтверджують і результати вивчення контенту вебсайтів органів місцевого самоврядування. Наприклад, на сайтах деяких міських, селищних, сільських рад, де заперечували роботу з вразливими даними, оприлюднені матеріали про діяльність адміністративних комісій, які обробляють вразливі персональні дані про притягнення членів місцевої громади до адміністративної відповідальності.

3.3. Організація внутрішнього контролю за захистом персональних даних

Стаття 24 Закону України *«Про захист персональних даних»* наголошує: *«володільці, розпорядники персональних даних зобов'язані забезпечити захист цих даних від випадкових втрати або знищення, від незаконної обробки, у тому числі незаконного доступу».* Згідно з підпунктами 3.1., 3.2. *«Типового порядку обробки персональних даних»,* захист має бути забезпечений на всіх етапах їх обробки, а володілець/розпорядник повинен *«самостійно визначити перелік і склад заходів, спрямованих на безпеку персональних даних».* Зрозуміло, що впровадження будь-яких заходів безпеки водночас має

передбачати обов'язковий контроль за їх виконанням, оскільки це дозволяє своєчасно виявити і швидко усунути проблеми у захисті персональних даних. Внутрішній контроль — це неодмінний компонент управлінської діяльності.

В даний час організація контролю за захистом персональних даних в органах місцевого самоврядування не витримує ніякої критики. Зі слів опитаних посадових осіб**,** у **94%** міських, селищних, сільських рад впродовж 2024 року **заходи з внутрішнього контролю за захистом персональних даних взагалі не здійснювалися.**

Жоден з 50 органів місцевого самоврядування, де проводився моніторинг, не надав документів, які б підтверджували виконання заходів з убезпечення персональних даних, передбачених *«Типовим порядком обробки персональних даних».* Зокрема до таких документів відносяться:

- перелік заходів, спрямованих на безпеку обробки персональних даних *(*підпункт 3.2. Типового порядку);
- аналітичні довідки щодо загроз безпеці персональних даних *(підпункт 3.18. Типового порядку)*;
- службові листи відповідальної особи з інформуванням керівництва органу про стан додержання законодавства про захист персональних даних *(підпункт 3.17. Типового порядку)*;
- службові листи відповідальної особи з інформуванням керівництва органу про виявлені порушення порядку обробки персональних даних та проведення заходів з їх усунення *(підпункт 3.18. Типового порядку)*;
- акти чи інші документи з фіксацією фактів порушень процесу обробки та захисту персональних даних *(підпункт 3.20. Типового порядку)*.

Фактична відмова посадових осіб від виконання функцій внутрішнього контролю насамперед зумовлена відсутністю необхідних для цього знань і навичок. За таких умов керівникам міських, селищних, сільських рад було б доцільно вдатися до проведення зовнішнього аудиту, у ході якого запрошені експерти можуть не тільки об'єктивно оцінити стан захисту персональних даних в органі, а й надати рекомендації щодо способів оптимізації цієї роботи, шляхів уникнення можливих інцидентів безпеки тощо. Проте такий аудит був проведений лише у **2 з 50** органів місцевого самоврядування.

3.4. Підготовка персоналу та просвітницька діяльність

Підвищення рівня кваліфікації та компетентності персоналу вважається одним з важливих напрямів управлінської діяльності, оскільки у будь-якій сфері отримання нових знань допомагає працівникам підвищити результативність своєї роботи. Підпункт 3.4. *«Типового порядку обробки персональних даних»*, поряд з іншими заходами з їх захисту, передбачає організацію *«**регулярного** навчання співробітників, які працюють з персональними даними».* Необхідність впровадження такого навчання в міських, селищних, сільських радах очевидна й безсумнівна, адже рівень захисту персональних даних напряму залежить від рівня обізнаності посадовців з відповідними вимогами законодавства.

Проте доводиться констатувати: очільники органів місцевого самоврядування ігнорують не тільки необхідність «регулярного навчання», а й навіть початкової підготовки персоналу. У **88%** міських, селищних, сільських рад впродовж 2024-2025 років заняття чи інші освітні заходи з питань захисту персональних даних з працівниками не проводились, у **98% —** не розроблений план (графік, програма) навчання з цієї тематики, у **94% —** відсутні методичні матеріали або конспекти для проведення занять. Одним із способів підвищення кваліфікації співробітників є залучення до проведення навчання експертів неурядових організацій, проте протягом 2024-2025 років лише у **4** міських, селищних, сільських рад **(8%)** скористались такою допомогою.

Експерти Асоціації вважають, що значна частина виявлених під час моніторингу прорахунків в організації захисту персональних даних мають місце саме через незадовільну виучку персоналу. На справедливість такого судження вказують і результати проведеного опитування посадових осіб, яке свідчить: посадовці погано орієнтуються як у базових вимогах законодавства у цій сфері, так і у конкретних питаннях створення безпечного інформаційного середовища безпосередньо в органі місцевого самоврядування. Наприклад, під час опитування чиновники часто повідомляли, що в їх радах з вразливими персональними даними не працюють, особисті відомості про громадян через офіційний вебсайт не отримуються, а автоматизовані системи у процесах обробки персональних даних не задіяні. Разом з тим моніторинг показав протилежне — в цих же радах діють адміністративні комісії, які збирають вразливі дані про осіб, притягнутих до адміністративної відповідальності, реєстраційні форми на сайтах для подання онлайн-звернень передбачають надання користувачами своїх персональних даних, а бухгалтерський та кадровий обліки автоматизовані.

Моніторинг виявив непоодинокі порушення **правил поширення персональних даних**, зокрема випадки оприлюднення на вебресурсах органів місцевого самоврядування вразливих персональних даних та таких, що стосуються сфери оборони. Серед іншого зафіксовані випадки публікування інформації про притягнення громадян до адміністративної відповідальності із зазначенням їх прізвища, імені та по батькові, адреси проживання та фабули вчиненого правопорушення. На сайті однієї з селищних рад у вільному доступі перебуває список, в якому вказані прізвища, ім'я та по батькові членів ініціативної групи зі створення місцевого добровольчого формування. На кількох сайтах розміщені списки осіб, які користуються пільгами при отриманні житла, влаштуванні дітей до дошкільних навчальних закладів тощо. При цьому у списках зазначені не тільки прізвища, імена, по батькові, адреси проживання та номери мобільних телефонів пільговиків, а й підстави для отримання ними пільг — *«учасник бойових дій», «учасник АТО», «інвалід-учасник АТО», «військовослужбовець у запасі», «працівник міліції», «співробітник ОВС», «співробітник ДСНС»*.

Безперечно, вебресурси органів місцевого самоврядування повинні максимально повно задовольняти інформаційні потреби громади, однак не за рахунок порушення права на приватність її окремих членів. Належне функціонування сайту має забезпечувати вузьке коло спеціально підготовлених і офіційно призначених осіб, на яких покладаються обов'язки з перевірки, а за потреби — редагування його контенту. Проте у **58%** міських, селищних, сільських рад співробітники, які відповідають за адміністрування сайту, відповідним документом не визначені.

Ще одним прикладом неуважного ставлення до збереження конфіденційності життя членів громади можна вважати існуючу в органах місцевого самоврядування практику **використання систем відеоспостереження.** Секретаріат Уповноваженого ВРУ з прав людини у 2021 році підготував *«Рекомендації щодо дотримання права на приватність під час встановлення і використання систем відеоспостереження у громадських місцях»,* проте моніторинг показав, що у більшості міських, селищних, сільських рад ці рекомендації залишили поза увагою. У **67%** населених пунктів зони здійснення відеоконтролю в громадських місцях не позначені попереджувальними знаками, а якщо такі знаки є, то **75%** з них не відповідають рекомендаціям до їх інформативного наповнення — на знаках відсутні відомості про те, ким здійснюється відеоспостереження та контактні дані відповідальної особи. У **85%** міських, селищних, сільських рад відсутня документація, що підтверджує відповідність використовуваних систем відеонагляду вимогам технічного захисту інформації (сертифікат відповідності, висновок за результатами експертизи тощо), у **83% —** не розроблений документ (окремий розділ у загальному документі), присвячений специфіці захисту персональних даних у мережах відеоспостереження. Посадові особи всіх органів місцевого самоврядування визнали, що впродовж 2023-2024 років жодних

заходів з контролю за безпекою обробки персональних даних у системах відеоспостереження не здійснювалось, а зовнішній (за участю запрошених експертів) аудит стану захисту інформації, отримуваної за допомогою мереж відеонагляду, не проводився.

Недостатній рівень правової підготовки посадовців зумовлює **недоліки в організації інформаційно-просвітницької роботи з населенням.** Відповідно до статей 8 та 12 Закону України *«Про захист персональних даних»*, суб'єкти персональних даних мають бути повідомлені про свої права, склад, зміст і місцезнаходження даних, джерела збирання і мету їх обробки, а також проінформовані про володільців/розпорядників персональних даних та третіх осіб, яким ці дані передаються. Результати моніторингу свідчать: системна робота з підвищення правової культури громадян у сфері захисту персональних даних в органах місцевого самоврядування майже не проводиться. Лише у **20%** міських, селищних, сільських рад на інформаційних стендах у вестибюлі адміністративної будівлі розміщена інформація про правові відносини, пов'язані з обробкою та захистом персональних даних. Дослідження змісту вебсайтів рад показало ще гіршу картину — тільки **14%** з них мають інформаційно-просвітницькі матеріали такої тематики.

4. Висновки та рекомендації

Рівень захищеності персональних даних в органах місцевого самоврядування слід розглядати як індикатор їх спроможності гарантувати дотримання прав і свобод членів громади, в тому числі як складової загальної інформаційної безпеки. Значні масштаби та широкий діапазон виявлених під час моніторингової кампанії порушень свідчать про те, що міські, селищні, сільські ради до виконання цієї функції наразі не готові.

Довготривала та виснажлива війна суттєво змінила пріоритети управлінської діяльності очільників органів місцевого самоврядування, яким довелося зосередитися на подоланні економічних і соціальних проблем воєнного часу, вкотре залишивши питання захисту персональних даних на периферії своїх інтересів. Запровадження воєнного стану не призвело до кардинального покращення рівня захисту персональних даних, а лише спонукало міські, селищні, сільські ради вдатися до додаткових обмежень у доступі громадян до інформації. Сумнівна дієвість такого підходу очевидна, оскільки непродумані й безпідставні заборони зазвичай створюють біль-

ше ризиків, аніж сприяють подоланню кризи. У нинішніх важких умовах війни керівникам органів місцевого самоврядування необхідно виконати складне, але цілком здійсненне завдання — швидко й всебічно посилити захист персональних даних, забезпечивши дотримання балансу інтересів: чиновників — у збереженні стабільності та ефективності управління, громадян — у недоторканості своїх базових прав та свобод.

Певною мірою досягненню цієї мети заважають недоліки законодавства, але вони аж ніяк не можуть бути виправданням управлінської інертності, оскільки навіть найдосконаліші нормативно-правові акти самі по собі не здатні розв'язати проблеми з захистом персональних даних. Проведений моніторинг ще раз підтвердив: захист персональних даних в органі місцевого самоврядування не в останню чергу залежить від рівня правової підготовки та активності посадових осіб, які мають повною мірою усвідомлювати значущість такої роботи для суспільства. Безграмотність, недбалість чи бездіяльність персоналу створюють не менше ризиків втрати та незаконного використання персональних даних, аніж цілеспрямовані дії ворога чи зловмисників.

Було б неправильно відкладати питання посилення контролю за обігом персональних даних на мирний час, як і сподіватися на можливість виправлення ситуації лише зусиллями Омбудсмана. Разом з тим, суттєво прискорити впровадження необхідних змін можливо завдяки поглибленню співпраці з громадським сектором. Вже сьогодні експерти неурядових організацій та підготовлені ними регіональні активісти готові допомогти органам місцевого самоврядування і взяти на себе частину організаційної та практичної роботи за кількома пріоритетними напрямками, зокрема:

— проводити незалежний аудит стану захисту персональних даних в міських, селищних, сільських радах з метою визначення причин можливого виникнення інцидентів безпеки та встановлення існуючих ризиків порушення прав членів громади;
— брати участь у заходах з підвищення правової підготовки персоналу, залученого до роботи з персональними даними;
— надавати відповідальним особам консультаційну, методичну та іншу підтримку у забезпеченні дієвого внутрішнього контролю за виконанням Закону України *«Про захист персональних даних»;*
— надавати адміністрації допомогу у розробці необхідних внутрішніх розпорядчих документів та сприяти зміцненню співробітництва з Офісом Омбудсмана.

Обнадійливим сигналом є те, що по завершенню моніторингу посадові особи більшості органів місцевого самоврядування заявляли про усвідомлення ними серйозності проблеми і демонстрували зацікавленість у зміні ситуації на краще. У **88%** міських, селищних, сільських рад посадовці визна-

ли необхідність термінового покращення рівня підготовки персоналу, при цьому найбільш затребуваними для проведення занять назвали наступні теми:

— *«Розробка внутрішньої документації з питань організації захисту персональних даних» (вважає 100% опитаних);*

— *«Вимоги національного законодавства у сфері захисту персональних даних» (вважає 86%);*

— *«Порядок взаємодії з Уповноваженим ВРУ з прав людини у питаннях захисту персональних даних» (вважає 64%);*

— *«Міжнародні стандарти захисту персональних даних» (вважає 57%).*

Загалом, посадові особи органів місцевого самоврядування під час моніторингу демонстрували прагнення до діалогу з громадськістю, готовність дослухатися до думки експертів та враховувати їхні рекомендації у практичній діяльності.

Окремо зазначимо, що у рамках кампанії працівникам міських, селищних, сільських рад надавалась консультаційна допомога, зокрема у питаннях планування заходів із захисту персональних даних, визначення можливих інцидентів безпеки, підготовки необхідної внутрішньої документації, налагодження співробітництва з Офісом Омбудсмана тощо.

З огляду на результати моніторингу, керівникам **органів місцевого самоврядування рекомендується:**

1. Для організації роботи, пов'язаної з захистом персональних даних при їх обробці, призначити відповідальну особу або створити відповідний структурний підрозділ *(стаття 24 Закону України «Про захист персональних даних»; підпункт 3.15 «Типового порядку обробки персональних даних», затвердженого наказом Уповноваженого ВРУ з прав людини від 08.01.2014 №1/02-14).*

Інформацію про зазначену відповідальну особу (структурний підрозділ) направити до Секретаріату Уповноваженого Верховної Ради України з прав людини для її подальшого оприлюднення *(стаття 24 Закону України «Про захист персональних даних»; підпункт 5.2. «Порядку повідомлення Уповноваженого ВР України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних при їх обробці, а також оприлюднення вказаної інформації», затвердженого наказом Уповноваженого ВРУ з прав людини від 08.01.2014 №1/02-14).*

2. Проаналізувати весь діапазон персональних даних, обіг яких здійснюється в органі, з метою виокремлення таких, чия обробка становить особливий ризик для прав і свобод громадян *(з урахуванням положень підпункту 1.2. «Порядку повідомлення Уповноваженого ВР України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних при їх обробці, а також оприлюднення вказаної інформації»).*

При наявності таких даних, повідомити про їх обробку Секретаріат Уповноваженого ВРУ з прав людини згідно з вимогами підпунктів 2.1 — 2.5 вищевказаного Порядку.

3. Проаналізувати стан нормативного врегулювання процесів обробки та захисту персональних даних в органі. З урахуванням положень Закону України *«Про захист персональних даних»,* а також директив і рекомендацій Уповноваженого ВРУ з прав людини, підготувати (актуалізувати) пакет внутрішніх розпорядчих документів у цій сфері. Зокрема, першочергово розробити:

3.1. ***«Політику щодо обробки персональних даних в органі місцевого самоврядування»,*** де сформулювати базові принципи й правила роботи з персональними даними та визначити:

- категорії суб'єктів персональних даних;
- склад персональних даних, мету і підстави їх обробки;
- спосіб збору і накопичення персональних даних, строки та умови їх зберігання;
- умови та процедури зміни, видалення або знищення персональних даних;
- умови та процедури їх передачі, а також перелік третіх осіб, яким персональні дані можуть передаватися;
- порядок доступу до персональних даних осіб, які здійснюють їх обробку, а також суб'єктів персональних даних;
- заходи з забезпечення захисту персональних даних;
- процедуру збереження інформації про операції, пов'язані з обробкою персональних даних та доступом до них;
- права й обов'язки суб'єктів відносин, пов'язаних із персональними даними.

(підпункти 2.1., 2.9. «Типового порядку обробки персональних даних»).

3.2. ***«Реєстр операцій з обробки персональних даних»,*** де фіксувати інформацію про всі операції, пов'язані з обігом персональних даних в органі. В реєстрі мають зберігатися відомості про:

— дату, час та джерело збирання персональних даних;

— зміну, перегляд, будь-яку їх передачу (копіювання);

— дату та час видалення або знищення персональних даних;

— мету та підстави зміни, перегляду, передачі та видалення або знищення персональних даних.

— працівника, який здійснив одну з вказаних операцій.

(підпункти 3.4., 3.11. «Типового порядку обробки персональних даних»).

3.3. ***«Посадову інструкцію відповідальної особи, яка організовує роботу, пов'язану з захистом персональних даних»,*** де визначити завдання, обов'язки, права, повноваження, зону відповідальності, період й порядок звітування відповідальної особи або керівника відповідного структурного підрозділу *(підпункти 2.2., 3.17. — 3.20. «Типового порядку обробки персональних даних»).*

3.4. ***«Облік працівників, які мають доступ до персональних даних»*** з встановленням рівня доступу кожного працівника *(підпункт 3.5. «Типового порядку обробки персональних даних»).*

3.5. ***«Письмове зобов'язання про нерозголошення персональних даних»,*** які було довірено (стали відомі) працівнику у зв'язку з виконанням професійних, службових або трудових обов'язків *(частина 3 статті 10 Закону України «Про захист персональних даних»; підпункт 3.7. «Типового порядку обробки персональних даних»).*

3.6. ***«Порядок доступу до персональних даних суб'єктів персональних даних»*** та ***«Порядок доступу до персональних даних працівників органу місцевого самоврядування»,*** в тому числі осіб, які здійснюють їх обробку *(підпункти 2.1., 3.4. «Типового порядку обробки персональних даних»).*

3.7. ***«План заходів із забезпечення захисту персональних даних»*** *(стаття 24 Закону України «Про захист персональних даних»; підпункти 2.1., 3.1. — 3.3. «Типового порядку обробки персональних даних»).*

3.8. ***«План дій на випадок несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, виникнення надзвичайних ситуацій»*** *(підпункт 3.4. «Типового порядку обробки персональних даних»).*

3.9. ***«План проведення занять з персоналом з тематики захисту персональних даних»*** *(підпункт 3.4. «Типового порядку обробки персональних даних»).*

3.10. ***«Реєстр порушень процесу обробки та захисту персональних даних»*** *(підпункт 3.20. «Типового порядку обробки персональних даних»).*

4. Проводити регулярні заслуховування звітів відповідальної особи (керівника структурного підрозділу) про стан виконання в органі вимог законодавства про захист персональних даних, дотримання прав громадян у цій сфері, а також про виявлені порушення та пропозиції з їх усунення і запобігання *(підпункти 3.17., 3.18 «Типового порядку обробки персональних даних»).*

5. Організувати регулярне навчання співробітників, які працюють з персональними даними. Для цього забезпечити відповідальну особу необхідними методичними матеріалами та технічними засобами для проведення занять у форматі онлайн. Впровадити практику запрошення для участі у навчанні персоналу експертів неурядових організацій *(підпункт 3.4. «Типового порядку обробки персональних даних»).*

6. Із залученням фахівців, перевірити наявні системи відеоспостереження та програмне забезпечення до них на відповідність вимогам інформаційної безпеки. Експлуатацію систем здійснювати з урахуванням *«Рекомендацій Уповноваженого ВРУ з прав людини щодо дотримання права на приватність під час встановлення і використання систем відеоспостереження у громадських місцях».*

7. Покращити рівень інформування членів громади про їх права як суб'єктів персональних даних. З цією метою:

7.1. На інформаційному стенді в адміністративній будівлі органу розмістити витяги з Закону України *«Про захист персональних даних»* щодо прав суб'єктів персональних даних (стаття 8), повноважень Уповноваженого ВРУ з прав людини у сфері захисту персональних даних (стаття 23), а також інформацію з контактними даними відповідальної особи (керівника структурного підрозділу);

7.2. Створити на сайті органу окрему вебсторінку *«Захист персональних даних»,* де опублікувати Закон України *«Про захист персональних даних»*, відповідні нормативні акти та рекомендації Уповноваженого ВРУ з прав людини, «Політику щодо обробки персональних даних в органі місцевого самоврядування», контактні дані відповідальної особи (керівника структурного підрозділу);

7.3. На вебсторінці сайту з формою для подання електронних звернень, які передбачають повідомлення заявником своїх персональних даних, розмістити гіперпосилання для переходу на вебсторінку *«Захист персональних даних».*

8. Проаналізувати вміст вебсайту органу з метою виявлення фактів оприлюднення інформації з персональними даними, які не підлягають поширенню. Провести знеособлення відкритих даних з урахуванням «Методичних рекомендацій для розпорядників інформації щодо деперсоніфікації наборів відкритих даних», підготовлених Міністерством цифрової трансформації України. Включити до посадових обов'язків відповідальної особи (працівника структурного підрозділу) здійснення контролю за змістом розміщуваного на сайті контенту з метою забезпечення його відповідності вимогам законодавства про захист персональних даних.

9. Розвивати партнерські відносини з неурядовими організаціями, потенціал яких можна використовувати для покращення захисту персональних даних. Запрошувати громадських експертів для надання ними консультативної та практичної допомоги у навчанні персоналу, розробці внутрішніх документів, проведенні аналізу стану захищеності персональних даних, визначенні загроз їх безпеці тощо.

Додаток

Дані щодо основних порушень нормативних актів у сфері захисту персональних даних та їх поширеності в органах місцевого самоврядування (у відсотках до загальної кількості охоплених моніторингом)

№	Виявлене порушення	Нормативний акт, вимоги якого порушено (не виконано)	Відсоток органів, де виявлені порушення
Організаційні заходи			
1	Не визначена відповідальна особа, яка організовує роботу, пов'язану із захистом персональних даних при їх обробці	Стаття 24 Закону України «Про захист персональних даних»; Підпункт 3.15. «Типового порядку обробки персональних даних» (затверджений наказом Уповноваженого ВРУ з прав людини від 08.01.2014 №1/02-14)	74%
2	Не визначені права та обов'язки відповідальної особи, призначеної для організації роботи із захисту персональних даних	Підпункт 2.2. «Типового порядку обробки персональних даних»	38%
3	Впродовж 2024 року не здійснювались заходи з внутрішнього контролю за захистом персональних даних	Стаття 24 Закону України «Про захист персональних даних»; Підпункти 3.1., 3.2. «Типового порядку обробки персональних даних»	94%
4	Від працівників не відбираються письмові зобов'язання про нерозголошення персональних даних, які їм було довірено або які стали їм відомі у зв'язку з виконанням професійних чи службових або трудових обов'язків	Стаття 10 Закону України «Про захист персональних даних»; Підпункт 3.7. «Типового порядку обробки персональних даних»	54%

Див. продовження таблиці на наступній сторінці

№	Виявлене порушення	Нормативний акт, вимоги якого порушено (не виконано)	Відсоток органів, де виявлені порушення
5	Суб'єкти персональних даних не повідомляються про свої права, визначені Законом України «Про захист персональних даних»	Стаття 12 Закону України «Про захист персональних даних»; Підпункт 2.9. «Типового порядку обробки персональних даних»	48%
6	Впродовж 2024-2025 років не проводилось навчання персоналу щодо вимог законодавства у сфері захисту персональних даних	Підпункт 3.4. «Типового порядку обробки персональних даних»	88%
Взаємодія з Уповноваженим ВРУ з прав людини			
7	Уповноваженому ВРУ з прав людини не направлено повідомлення про призначення відповідальної особи, яка організовує роботу, пов'язану із захистом персональних даних при їх обробці	Стаття 24 Закону України «Про захист персональних даних»; Підпункт 3.16. «Типового порядку обробки персональних даних» (затверджений наказом Уповноваженого ВРУ з прав людини від 08.01.2014 №1/02-14); Пункт 5 «Порядку повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних при їх обробці, а також оприлюднення вказаної інформації» (затверджений наказом Уповноваженого ВРУ з прав людини від 08.01.2014 №1/02-14)	77%

Див. продовження таблиці на наступній сторінці

№	Виявлене порушення	Нормативний акт, вимоги якого порушено (не виконано)	Відсоток органів, де виявлені порушення
8	Уповноваженому ВРУ з прав людини не направлено повідомлення про здійснення обробки персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних	Стаття 9 Закону України «Про захист персональних даних»; Пункт 2 «Порядку повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних при їх обробці, а також оприлюднення вказаної інформації»	83%
Службова документація			
9	Відсутня «Політика щодо обробки персональних даних»	Пункти 1,2 «Типового порядку обробки персональних даних»	62%
10	Відсутній «Реєстр обробки персональних даних»	Підпункт 2.1., 3.4., 3.11. «Типового порядку обробки персональних даних»	80%
11	Відсутній «План дій на випадок несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, виникнення надзвичайних ситуацій»	Підпункт 3.4. «Типового порядку обробки персональних даних»	74%
12	Відсутній документ, який визначає строки та умови зберігання персональних даних різних категорій	Підпункт 2.1. «Типового порядку обробки персональних даних»	76%
13	Відсутній документ, який встановлює процедуру зміни, знищення або видалення персональних даних по закінченню строку їх зберігання	Підпункт 2.1. «Типового порядку обробки персональних даних»	76%
14	Відсутній документ, який фіксує факт знищення/видалення персональних даних (акти знищення, відповідні записи у реєстрі чи журналі)	Підпункт 3.11. «Типового порядку обробки персональних даних»	76%

Див. продовження таблиці на наступній сторінці

№	Виявлене порушення	Нормативний акт, вимоги якого порушено (не виконано)	Відсоток органів, де виявлені порушення
15	Відсутній документ з переліком третіх осіб, яким можуть бути передані персональні дані, та визначенням умов і процедури такої передачі	Підпункт 2.1. «Типового порядку обробки персональних даних»	86%
16	Відсутній облік працівників, які мають доступ до персональних даних	Підпункт 3.5. «Типового порядку обробки персональних даних»	80%
17	Відсутні посадові інструкції для працівників, залучених до обробки персональних даних	Підпункти 2.1., 3.4. «Типового порядку обробки персональних даних»	70%
18	Відсутній документ з переліком і складом заходів, спрямованих на безпеку обробки та захист персональних даних	Підпункти 2.1., 3.2. «Типового порядку обробки персональних даних»	100%
19	Відсутні аналітичні довідки щодо загроз безпеці персональних даних	Підпункт 3.18. «Типового порядку обробки персональних даних»	100%
20	Відсутні службові листи відповідальної особи з інформуванням керівництва про стан додержання законодавства про захист персональних даних	Підпункт 3.17. «Типового порядку обробки персональних даних»	100%
21	Відсутні службові листи відповідальної особи з інформуванням керівництва про виявлені порушення порядку обробки персональних даних та проведення заходів з їх усунення	Підпункт 3.18. «Типового порядку обробки персональних даних»	100%
22	Відсутні акти чи інші документи з фіксацією фактів порушень процесу обробки та захисту персональних даних	Підпункт 3.20. «Типового порядку обробки персональних даних»	100%

-

Для нотаток


Freerights
ASSOCIATION