ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В ОРГАНАХ МІСЦЕВОГО САМОВРЯДУВАННЯ:

стандарти і кроки впровадження

2022

Асоціація
УМДПЛ
UMDPL
Association

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В ОРГАНАХ МІСЦЕВОГО САМОВРЯДУВАННЯ: стандарти і кроки впровадження / У. Шадська, Т. Олексіюк, В. Батчаєв. — Київ: Асоціація УМДПЛ, 2022. — 58 с.

Цей матеріал — своєрідний путівник для органів місцевого самоврядування, розроблений для того, щоб допомогти організувати роботу у сфері захисту персональних даних відповідно до вимог законодавства. Зміст цього документа можна використовувати для проведення навчальних та інших просвітницьких заходів.

Ідея та упорядкування:
Уляна Шадська

Авторський колектив:
Уляна Шадська, Тетяна Олексіюк, Володимир Батчаєв

Літературне редагування:
Мар'яна Добоні

Дизайн:
Ольга Золотар

Посібник підготовлено за підтримки Міжнародного Фонду «Відродження» та Європейського Союзу в рамках гуманітарної ініціативи «Людяність і взаємодопомога». Матеріал відображає позицію авторів і не обов'язково відображає позицію Міжнародного фонду «Відродження» та Європейського Союзу».

ПРЯМУЄМО РАЗОМ

Європейський Союз складається з 28 держав-членів та їхніх народів. Це унікальне політичне та економічне партнерство, засноване на цінностях поваги до людської гідності, свободи, рівності, верховенства права і прав людини. Понад п'ятдесят років знадобилось для створення зони миру, демократії, стабільності і процвітання на нашому континенті. Водночас нам вдалось зберегти культурне розмаїття, толерантність і свободу особистості. ЄС налаштований поділитись своїми цінностями та досягненнями з країнами-сусідами ЄС, їхніми народами, та з народами з-поза їхніх меж.

МІЖНАРОДНИЙ ФОНД ВІДРОДЖЕННЯ

Міжнародний фонд «Відродження» – одна з найбільших благодійних фундацій в Україні, що з 1990-го року допомагає розвивати в Україні відкрите суспільство на основі демократичних цінностей. За час своєї діяльності Фонд підтримав близько 20 тисяч проектів, до реалізації яких долучилися понад 60 тисяч активістів та організацій України на суму понад 200 мільйонів доларів США.

Сайт: **www.irf.ua**

Facebook: **www.fb.com/irf.ukraine**

Зміст

Передмова

На різноманітних заходах за участі представників і представниць державних органів влади та місцевого самоврядування часто можна помітити, що коли починається обговорення питання захисту персональних даних, навіть у найбадьорішої аудиторії змінюється настрій. І це можна зрозуміти. Кожен, хто стикався з питаннями, які стосуються права людини на приватність, розуміє, який необхідний обсяг знань, щоб з цим розібратися та правильно дотримуватися відповідного законодавства. Окрім застосування положень Закону України «Про захист персональних даних», який рясніє специфічними термінами та визначеннями, треба вміти оперувати міжнародними стандартами забезпечення цього права та вивчати прецеденти судової практики.

Те, що це не формальність, а надзвичайно важливі питання для системи державного управління, навіть у сфері національної безпеки, довели події, пов'язані з російською військовою агресією в Україні. Зокрема, коли окупанти за допомогою баз, які містять персональні дані, у тому числі володільцями яких є органи місцевого самоврядування, розшукують потрібних їм людей. Предметом зацікавленості можуть бути власники бізнесу, місцеві чиновники, активісти громадських об'єднань, військові та правоохоронці, власники зброї, журналісти. Цей список може бути продовжений залежно від цілей і завдань, які поставить ворог своїм спецслужбам.

Витік конфіденційної інформації відбувається не лише під час війни, випадки несанкціонованого доступу до особистих даних і їх подальше неправомірне використання траплялися і в мирний час. Якщо раніше порушення права на захист персональних даних мало більше латентний характер, то під час військової агресії добре видно наслідки для життя людини та держави загалом. Також негативні прецеденти, які бачимо сьогодні, не завжди пов'язані з проблемами технічного захисту систем, часто це наслідки так званої соціальної інженерії, коли завдана шкода для інтересів держави або окремих осіб стала результатом звичайної недбалості, правової безграмотності або нехтування елементарними правилами «інформаційної гігієни» з боку посадових осіб, відповідальних за безпеку такої інформації, які повинні робити все можливе, щоб мінімізувати ризики витоку інформації.

З часом нам ще доведеться детальніше розібратися з наслідками недотримання законодавства у сфері захисту персональних даних, але вже зараз маємо достатньо аргументів для того, щоб терміново працювати над тим, щоб якомога швидше виправити цю ситуацію. Для цього нам потрібно

передусім впровадити базові вимоги закону й забезпечити ефективні й сталі практики його безумовного виконання.

Саме для цього команда юристів — Уляна Шадська, Тетяна Олексіюк і Володимир Батчаєв — у межах проєкту Асоціації УМДПЛ, що реалізується за підтримки Міжнародного фонду «Відродження», розробила методичний матеріал у форматі своєрідної «дорожньої карти» необхідних кроків для організації та забезпечення захисту персональних даних. Це видання не обтяжене складними термінами та призначене насамперед для практиків, які опікуються питаннями захисту інформації під час своєї повсякденної діяльності в органах державної влади та місцевого самоврядування.

З повагою

Вадим Пивоваров,
виконавчий директор Асоціації українських моніторів
дотримання прав людини в діяльності правоохоронних органів

Загальна частина

1. Чому важливо розібратися у сфері захисту персональних даних?

Сучасна тенденція цифрової трансформації торкнулася не тільки центральних органів виконавчої влади, а й органів місцевого самоврядування (далі — ОМС), які здійснюють управління справами в інтересах певної територіальної громади. Повноваження виконавчих органів сільських, селищних, міських рад стосуються різних галузей — житлово-комунального господарства, освіти, охорони здоров'я, соціального захисту населення, оборони, бюджету, забезпечення правопорядку тощо. Виконання завдань зумовлює необхідність збирати та обробляти значні обсяги персональних даних населення.

З кожним роком в ОМС ухвалюються нові технологічні рішення для вдосконалення своєї діяльності: впроваджуються системи електронного документообігу; відеоспостереження для підтримки публічної безпеки; створюються вебсайти, онлайн-послуги для мешканців тощо. Стрімкий розвиток технологій, окрім переваг, водночас створює великий спектр ризиків для недоторканності приватного життя людини. Ці загрози суттєво збільшуються у воєнний час, коли витоки персональних даних можуть становити загрозу життю та здоров'ю людей.

За таких умов належний захист особистої інформації стає важливим критерієм довіри громади до ОМС, адже приватність людини напряму стосується в тому числі її фізичної безпеки. Питання необхідності встановлення чітких правил роботи з персональними даними набуває все більшої актуальності. Кожний ОМС повинен довести місцевій громаді свою спроможність забезпечити належний захист інформації, яку йому довірили, а для цього потрібно розібратися із законодавством, врахувати особливості застосування нових технологій, розмежувати публічне та приватне.

Як же цього досягнути?

Одразу зазначимо, що немає єдиного універсального шаблону, як організувати роботу з персональними даними, оскільки діяльність кожного ОМС має свою специфіку залежно від внутрішньої структури, чисельності штату тощо. Але існують базові вимоги, передбачені законом і міжнародними стандартами, які необхідно запровадити для надійного збереження інформації.

> Усі ідеї та доробки проходили через фільтр основного бенефіціара

2. Про які проблеми захисту персональних даних ми дізналися?

На початку 2022 року команда проєкту проводила зустрічі[1] з представниками ОМС з різних регіонів України для того, щоб зрозуміти, з якими саме проблемами вони стикаються під час обробки персональних даних. Це дало змогу визначити перелік основних питань, що й стали предметом розгляду в цьому методичному матеріалі.

Як виявилося, більшість проблем були пов'язані з організаційними процесами обробки даних і відсутністю внутрішнього контролю. Під час розмови службовці визнавали, що потребують підвищення кваліфікації для кращого розуміння положень законодавства в цій сфері. Зазвичай розв'язання питань, пов'язаних із персональними даними, віднесене до компетенції відділів діловодства, управлінь юридичного забезпечення або інформаційно-комп'ютерних підрозділів. Лише невелика кількість працівників цих підрозділів відвідувала спеціалізовані навчальні заходи. Водночас до повсякденної роботи, напряму пов'язаної з персональними даними (надання муніципальних послуг, організація діяльності комунальних підприємств, створення різноманітних реєстрів, ведення журналів тощо), залучається значно більша кількість персоналу. Ці співробітники несуть відповідальність за належне зберігання і використання інформації, але відповідного навчання взагалі не проходили.

Персональні дані в ОМС можуть зберігатися як на папері, так і в інформаційних системах або на інших носіях. Оскільки сьогодні майже вся інформація оцифровується, ризик витоку даних в електронній формі значно вищий. При цьому загрозу може становити, як зовнішній злам системи з віддаленого комп'ютера (так звана хакерська атака), так і недбалість чи навмисні дії з боку службовців ОМС, тобто коли до протиправного поширення даних причетні самі працівники.

Також ми з'ясували, що порівняно невелика кількість ОМС розробила та впровадила внутрішні розпорядчі документи, які регулюють питання у цій сфері. Навіть у тих ОМС, які ухвалили внутрішні політики у сфері приватності, такі документи часто були скопійовані з інших ресурсів і не адаптовані до діяльності конкретної установи. Відсутність внутрішньої регуляції всіх процесів роботи з даними призводить до ризиків — від порушення загального циклу їх обробки до можливого витоку інформації.

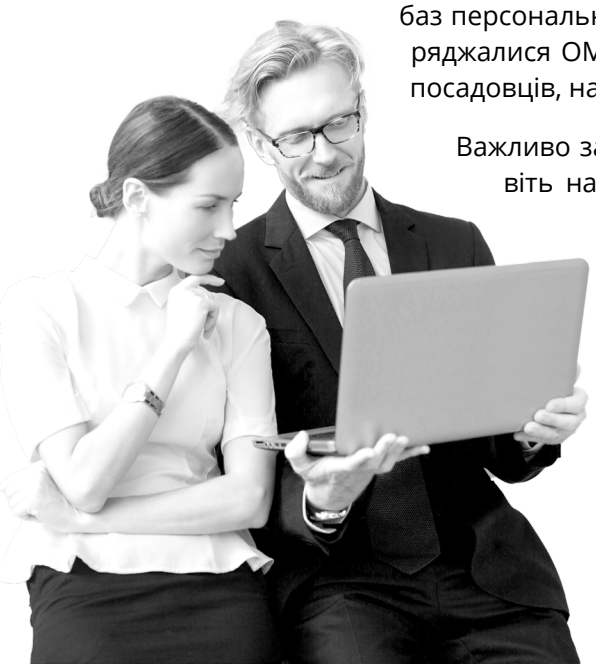
1 Онлайн-зустрічі, а також опитування за допомогою телефонних інтерв'ю і письмових анкет (січень 2022 року).

Лишаються неврегульованими також питання збору інформації та її зберігання. Частими є випадки, коли ОМС накопичують надлишковий обсяг інформації, що заважає її систематизації для використання із запланованою метою. Ще однією поширеною проблемою є агрегація даних. Об'єднання різних баз даних в єдину становить ризики як для організації внутрішнього управління (ускладнює виконання вимог закону, наприклад диференціацію інформації або вчасне видалення даних), так і для особи, чия інформація міститься у базах даних, адже це може призвести до небажаної ідентифікації людини через її загальний профайл.

У відділах кадрів, діловодства та архівах зберігаються особові справи працівників ОМС і депутатів місцевих рад, які містять, окрім їхніх особистих даних, ще відомості про склад сім'ї тощо. Здебільшого в ОМС не організовані безпечні умови обробки спеціальної категорії даних, які можуть становити особливі ризики для людини — небезпеку переслідування, тиску, фізичної розправи або порушення інших прав та свобод. Практично жоден ОМС не проводив роботи з оцінювання ризиків у сфері обробки даних. Про це детальніше розповімо далі.

Переважна частина проблем, з якими стикнулися ОМС у воєнний час, не є новою або притаманною лише сьогоденню. Недоліки в організації роботи із захисту персональних даних існували й до повномасштабної війни, проте саме виклики воєнного часу загострили їх, почасти зробивши їх такими, що безпосередньо впливають на життя та безпеку людини.

Завдану шкоду й негативний вплив на ситуацію в країні внаслідок неналежного захисту персональних даних в ОМС під час військової агресії оцінювати складно. Однак численні повідомлення у ЗМІ свідчать про те, що окупанти постійно намагаються отримати доступ до баз персональних даних, у тому числі тих, якими розпоряджалися ОМС, не гребуючи для цього викраденням посадовців, насильницькими діями й шантажем.



Важливо зауважити, що нас приємно вразила й навіть надихнула зацікавленість учасників зустрічей здобути нові знання, їх розуміння актуальності проблеми й серйозність ставлення до власного професійного зростання. Після тривалих обговорень і дискусій наша команда дійшла висновку, що цей методичний матеріал доцільно побудувати з трьох розділів, перший з яких присвятити

теоретичним засадам, а другий і третій — відповідям на питання про процеси обробки персональних даних і їх захист.

Ми прагнули висвітлити різні аспекти проблем захисту персональних даних та у форматі «питання — відповідь» показати, як саме можна змінити ситуацію. Ми свідомо відмовилися від ускладнення тексту детальним експертним аналізом нормативних актів чи розбором практики їх правозастосування. Також не керувалися хибним, на нашу думку, принципом «що товстіша брошура, то вона солідніша». Для нас важливіше було створити якісний, але доступний для мотивованого читача матеріал, однаково зручний як для самостійного вивчення, так і використання під час проведення навчальних заходів з працівниками ОМС.

Сподіваємося, нам це вдалося, і ця Дорожня карта допоможе налагодити ефективну роботу всіх структурних підрозділів ОМС, які обробляють персональні дані, а також сприятиме конструктивній співпраці між посадовими особами, відповідальними за доступ до інформації, і тими, хто відповідатиме за захист персональних даних.

> **Формування безпечнішого цифрового майбутнього — стратегія в новому десятилітті**

РОЗДІЛ І
ОСНОВНІ ПОЛОЖЕННЯ ЗАКОНОДАВСТВА

Для виконання своїх повноважень ОМС збирають різну інформацію, значна частина якої містить персональні дані. Щоб з'ясувати, чи дотримуються вимоги закону щодо їх обробки, насамперед необхідно розібратися зі змістом термінів і правил, які в ньому визначені.

1. Що таке персональні дані?

У Законі України *«Про захист персональних даних»* визначено, що персональні дані — це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

Зверніть увагу, закон не наголошує на тому, що всі відомості про людину є її персональними даними. Вичерпного переліку таких даних узагалі не існує і до них відносять лише ту інформацію, яка дає можливість встановити особу: ПІБ, паспортні дані, ідентифікаційний номер, банківський рахунок, номер особистого телефона, біометричні дані тощо.

Доволі часто для проведення ідентифікації людини вирішальне значення мають не окремі дані, а їх сукупність. Приміром, вивішене на інформаційному стенді біля будинку оголошення *«Власник квартири № 13 має заборгованість зі сплати комунальних послуг»* не розголошує персональні дані, але зазначення номера квартири або прізвища та імені створює умови для встановлення особи боржника *(непряма ідентифікація).*

Ще приклад.

Особа відвідала комунальну спеціалізовану медичну клініку, де на умовах анонімності отримала консультацію в лікаря. Здавалося б, ситуація аж ніяк не становить загрози для персональних даних відвідувача, адже його особа залишилася невстановленою. Проте все кардинально змінюється, якщо на автостоянці встановлені камери відеоспостереження, а оплата була проведена за допомогою банківської картки. У такому випадку факт надання медичної допомоги персоналізується, оскільки з'являється інформація про те, хто конкретно, на якому авто відвідав лікаря, а з урахуванням спеціалізації клініки можна робити певні висновки про стан здоров'я особи. Отже, медична установа зобов'язана забезпечити захист отриманих відомостей, які разом є персональними даними.

Важливо, щоб відповідальні особи ОМС, які працюють з персональними даними, розуміли різницю між персональними даними та конфіденційною інформацією, адже ці поняття не є тотожними. Відповідно до Закону України *«Про доступ до публічної інформації»* конфіденційною є інформація, доступ до якої обмежено фізичною або юридичною особою, окрім суб'єктів владних повноважень, і яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов. Слід взяти до уваги, що тільки особи приватного права можуть вирішувати, яка інформація про них є конфіденційною, а яка відкритою.

Персональні дані завжди стосуються фізичної особи незалежно від її віку та дієздатності. Інформація про померлу особу не є її персональними даними, хоча може бути визнана конфіденційною. Так, у статті 7 Закону України *«Про поховання та похоронну справу»* закріплено, що держава гарантує конфіденційність інформації про померлого. Водночас до конфіденційної може належати також інформація про юридичну особу, наприклад комерційна таємниця. Відповідно до статті 505 Цивільного кодексу України це можуть бути відомості технічного, організаційного, комерційного, виробничого та іншого характеру (за винятком тих, які відповідно до закону не можуть бути віднесені до комерційної таємниці) і щодо яких ця юридична особа вжила заходи зі збереження секретності.

Більш детально розглянемо це питання в окремому пункті про правила обмеження доступу до інформації, зокрема конфіденційної.

2. Які є види та категорії персональних даних?

Існують дві категорії персональних даних — загальна та особлива (її ще називають чутливою). Законодавець розділяє інформацію на категорії, оскільки поширення чутливої інформації може становити особливий ризик для прав і свобод людини. Наприклад, до загальної категорії можна віднести прізвище та ім'я, інформацію про місце народження та проживання; дані, записані в посвідченні водія; підпис; IP-адреси тощо.

Перелік персональних даних, які відносять до особливої категорії, чітко визначений і є вичерпним (на відміну від загальної категорії). Це інформація про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях і професійних спілках, засудження до кримінального покарання, а також відомості, що стосуються здоров'я, статевого життя, біометричних або генетичних даних[2].

2 Стаття 7 Закону України «Про захист персональних даних».

3. Коли приватна інформація може ставати відкритою?

Це питання хвилює багатьох не просто так, адже мова йде про «червоні лінії» приватності. Закон поділяє інформацію на відкриту та з обмеженим доступом[3]. Своєю чергою одним з видів інформації з обмеженим доступом є інформація конфіденційна. Вона стосується даних про фізичну особу або в окремих випадках особу юридичну.

Персональні дані можуть бути віднесені до конфіденційної інформації, але не завжди. Наприклад, закон забороняє відносити до конфіденційної інформації:

— персональні дані особи, яка обіймає посаду, пов'язану з виконанням функцій держави або ОМС;

— відомості, зазначені в декларації особи, яка подається відповідно до Закону України *«Про запобігання корупції»*;

— дані про умови отримання, користування, володіння чи розпорядження державним, комунальним майном або коштами. Не підлягає обмеженню інформація про стан і результати перевірок або розслідувань у цих сферах.

Запровадження подібних обмежень не означає, що чиновники не мають права на приватне життя. Просто офіційний статус осіб повинен передбачати певні правові обтяження, які будуть наочно демонструвати суспільству доброчесність посадовців і формувати довіру до влади. Зрозуміло, що кожний випадок, пов'язаний з визначенням рівня конфіденційності життя людини, повинен розглядатися окремо, оскільки дотримання балансу між відкритістю та приватністю залежить від багатьох факторів.

Що стосується поширення даних, віднесених до категорії чутливих, слід узяти до уваги положення постанови Пленуму Вищого адміністративного суду України від 29 вересня 2016 року № 10 *«Про практику застосування адміністративними судами законодавства про доступ до публічної інформації»*, у якій узагальнена судова практика щодо віднесення інформації до конфіденційної. У пункті 6.4 цієї постанови наведено правило врахування вагомого суспільного інтересу в отриманні інформації, у тому числі персональних даних:

«7) лише дуже серйозні доводи на користь суспільного інтересу в розголошенні інформації можуть переважити можливу шкоду інтересам захисту права на невтручання в особисте життя та захисту персональних даних,

3 Стаття 20 Закону України «Про інформацію».

коли йдеться про так звані вразливі персональні дані (дані про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та професійних спілках, засудження до кримінального покарання, а також дані, що стосуються здоров'я, статевого життя, біометричних або генетичних даних)».

Простіше кажучи, інтереси суспільства вищі за інтереси окремої особи й за наявності незаперечного суспільного інтересу, підтвердженого наведенням вагомих доводів, можливе розкриття навіть чутливих персональних даних.

У будь-якому випадку обмеження доступу до персональних даних посадових осіб ОМС слід керуватися в тому числі частиною 2 статті 6 Закону України *«Про доступ до публічної інформації»*, яка зобов'язує застосовувати так званий трискладовий тест і належним чином обґрунтовувати своє рішення.

Для того, щоб отримати більше інформації про те, як має відбуватися обмеження доступу до інформації про діяльність ОМС, рекомендуємо звернутися до спеціального посібника із застосування трискладового тесту[4] та судової практики.

***Примітка**. Для поглибленого ознайомлення з цим питанням варто вивчити окремі правові норми, зокрема:*

1. *загальні положення щодо інформації з обмеженим доступом — стаття 21 Закону України «Про інформацію»;*
2. *коли персональні дані можуть бути віднесені до конфіденційної інформації та винятки — стаття 5 Закону України «Про захист персональних даних»;*
3. *порядок віднесення інформації до конфіденційної — стаття 6 Закону України «Про доступ до публічної інформації».*

4. Що таке обробка персональних даних?

З цим усе просто. Обробка персональних даних — це будь-яка дія з даними, від їх збирання до знищення. Тобто реєстрація, накопичення, зберігання, адаптування, зміна, оновлення, використання, поширення (розповсюдження, реалізація, передача), знеособлення тощо[5] — усе це види обробки персональних даних.

4 Публічна інформація: посібник із застосування трискладового тесту. Режим доступу: http://eidos.org.ua/vydannya/posbinyk-publichna-informatsiya-posbibnyk-iz-zastosuvannya-tryskladovoho-testu/

5 Стаття 2 Закону України «Про захист персональних даних».

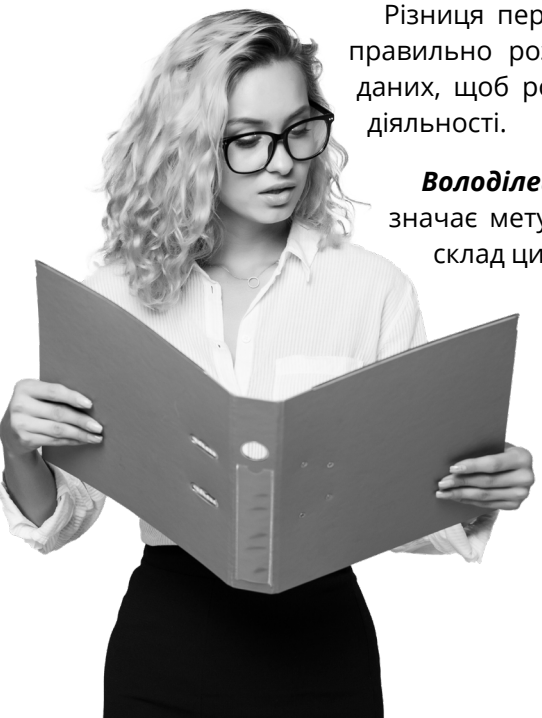
Наприклад, претендент на посаду заповнив анкету зі своїми даними та резюме, після чого віддав їх у підрозділ по роботі з персоналом. Своєю чергою працівник кадрового відділу не просто отримав документи для ухвалення рішення про можливість працевлаштування, а приступив до обробки персональних даних кандидата, адже збирання відомостей про людину вважається одним з етапів такої обробки.

5. Чи потрібно враховувати категорію даних під час їх обробки?

Обов'язково. Адже саме від категорії даних залежить вибір тих чи інших рівнів безпеки, які мають бути застосовані при їх обробці. Зрозуміло, що необхідно керуватися принципом «що серйозніша загроза, то міцніший захист». Оскільки втрата даних особливої категорії становить більшу небезпеку, то й заходи для їх захисту мають бути ретельнішими.

Законодавство передбачає, що в разі обробки таких даних необхідно повідомити Уповноваженого Верховної Ради України з прав людини про структурний підрозділ або відповідальну особу, яка організовує роботу з ними. Про те, яким чином це потрібно зробити, можна дізнатися на офіційному сайті Уповноваженого.

6. Володілець і розпорядник[6] персональних даних: у чому різниця?



Різниця передусім у повноваженнях, а отже, необхідно правильно розрізняти суб'єктів, які залучені до обробки даних, щоб розуміти зони їх відповідальності й напрями діяльності.

Володілець — фізична або юридична особа, яка визначає мету обробки персональних даних, встановлює склад цих даних і процедури їх обробки, якщо інше не визначено законом.

Розпорядник — фізична чи юридична особа, якій володільцем персональних даних або законом надано право обробляти ці дані від імені володільця.

6 Відповідно до європейського законодавства — контролери й процесори.

Для наочності наведемо індикатори, за якими можна відрізнити *«володільця»* від *«розпорядника»* персональних даних.

	Володілець	Розпорядник
1.	Першочергово збирає персональні дані	Отримує дані від володільця
2.	Визначає правові підстави, цілі та порядок обробки даних	Обробляє дані лише з тією метою, яка була визначена володільцем, якщо інше не передбачено законом
3.	Самостійно вирішує, кому будуть передані дані (відповідно до закону чи інших нормативних актів)	Обробляє інформацію лише в межах договору з володільцем або профільного закону
4.	Має право укладати угоди про передачу або обмін даними від свого імені	Діє лише в межах договору з володільцем, якщо інше не передбачено законом
5.	Визначає строки зберігання та порядок видалення даних	Діє лише в межах договору з володільцем, якщо інше не передбачено законом

Слід пам'ятати й про те, що визначення розпорядника персональних даних (відповідно до законодавства про захист персональних даних) і розпорядника публічної інформації (відповідно до Закону України *«Про доступ до публічної інформації»*) суттєво відрізняється.

7. Для яких цілей можна обробляти персональні дані?

Мета обробки персональних даних має бути сформульована в законах, інших нормативно-правових актах, положеннях, установчих чи документах, які регулюють діяльність володільця даних, і відповідати законодавству. Загальний процес роботи з даними повинен здійснюватися відкрито й прозоро. Тобто мають бути обґрунтовані правові підстави збору конфіденційної інформації та подальшої роботи з нею.

8. Які правові підстави обробки персональних даних?

Підстави[7] обробки персональних даних:

1. згода суб'єкта персональних даних;
2. дозвіл на обробку персональних даних, наданий їх володільцю відповідно до закону лише для здійснення його повноважень;
3. укладення та виконання правочину, стороною якого є суб'єкт персональних даних або який укладено на користь суб'єкта персональних даних чи для здійснення заходів, що передують укладенню правочину на вимогу суб'єкта персональних даних;
4. захист життєво важливих інтересів суб'єкта персональних даних;
5. необхідність виконання обов'язку володільця (наприклад, ОМС) персональних даних, який передбачений законом;
6. необхідність захисту законних інтересів володільця персональних даних або третьої особи, якій передаються дані, окрім випадків, коли потреби захисту основоположних прав і свобод суб'єкта персональних даних у зв'язку з їх обробкою переважають такі інтереси.

Згода людини на обробку персональних даних не отримується як виняток і лише в тих випадках, коли збір інформації прямо передбачений законом і необхідний для виконання обов'язку володільця персональних даних. Водночас саме собою існування таких повноважень є недостатньою умовою для обробки даних — має бути обґрунтована мета та процедура, визначена у внутрішній розпорядчій документації.

9. Як визначити необхідний обсяг персональних даних?

Необхідно керуватися принципами раціональності та доцільності, жодних роздумів на кшталт *«запас кишеню не обтягне»* чи *«а може, у майбутньому згодиться».*

До того ж законодавство наполягає: персональні дані повинні оброблятися тільки за наявності правових підстав та обмежуватися тим обсягом, який необхідний для досягнення конкретно визначеної мети їх обробки.

7 Стаття 11 Закону України «Про захист персональних даних».

Отже, передусім слід відповісти собі на такі питання:

1. *Чи достатньо чітко визначено мету та завдання обробки даних?*
2. *Чи збираються дані тільки для досягнення конкретних і заздалегідь визначених цілей (чи не збираються надлишкові дані)?*
3. *Чи здійснюється аналіз обсягу даних?*
4. *Чи передбачена процедура видалення надлишкових даних і тих, потреби в яких більше немає?*

10. Що таке накопичення даних і який термін їх зберігання?

Накопичення даних передбачає дії щодо поєднання та систематизації відомостей про фізичну особу чи групу фізичних осіб або внесення їх до відповідних баз. У цьому процесі спосіб ролі не грає: автоматичне упорядковування файлів на жорсткому диску, влиття карток в картотеку обліку чи просто розподілення паперових анкет по папках-накопичувачах — це все накопичення даних.

Зберігання даних передбачає дії щодо забезпечення їх цілісності та відповідного режиму доступу до них[8]. Наказом Міністерства юстиції України від 12 квітня 2012 року № 578/5 затверджений *Перелік типових документів, що створюються під час діяльності державних органів, інших установ, підприємств та організацій*, із зазначенням строків зберігання документів.

Зберігання даних на будь-яких носіях передбачає дії щодо забезпечення їх цілісності та відповідного режиму доступу до них протягом певного строку. Вони повинні зберігатися не довше, ніж це необхідно для досягнення поставлених цілей, якщо інше не передбачено законом. Далі дані автоматично знищуються або передаються в архів. В окремих випадках строк зберігання може бути продовжено, але це має бути обґрунтовано та визначено у відповідних внутрішніх розпорядчих документах.

8 Стаття 13 Закону України «Про захист персональних даних».

РОЗДІЛ ІІ
ОРГАНІЗАЦІЙНІ ЗАХОДИ ТА ВНУТРІШНІЙ КОНТРОЛЬ

Уявіть собі, що у вас перший робочий день в ОМС і перед вами стоїть завдання впорядкувати персональні дані в структурному підрозділі або установі загалом. Багато хто подумає, що для цього достатньо просто завантажити в інтернеті шаблон політики приватності, вписати туди деякі дані та опублікувати на офіційному сайті.

Але такий підхід немає нічого спільного з організацією захисту інформації відповідно до законодавства. У багатьох випадках процес збору й накопичення даних можна порівняти з шафою і речами. Декілька років вона завантажувалася потрібними або непотрібними речами (персональними даними). Ніхто їх не прибирав, не систематизував, не контролював до них доступ, використання, розповсюдження тощо. І взагалі не замислювалися, що це потрібно робити, продовжуючи завантажувати, завантажувати...

Одного дня вирішили навести лад. У цьому випадку потрібно виконати такі завдання:

1. Ознайомити свою команду, чому це потрібно (вимоги законодавства).
2. Провести аудит. Розібратися, хто, що й навіщо збирав, у якій кількості, що треба залишити, а що знищити.
3. Роздивитися свою шафу, чи вона має потрібні полиці, щоб обмежити доступ до делікатних речей (спеціальних даних), інші розкласти так, щоб було зрозуміло їх використання. Потім ще раз проаналізувати, що насправді потрібне, а що зайве.
4. За результатами аудиту розробити внутрішні політики, які повинні щонайменше включати архітектуру інформаційних систем, програм, кількість осіб, які мають до них доступ. Ось тепер можна врегулювати процедури, розуміючи ціль, обсяг, категорії, порядок збору, доступу, відповідальність за поширення та зберігання даних тощо.

Тепер уже краще зрозуміло, чому «шаблон» не розв'яже проблему, а потрібний індивідуальний і комплексний підхід. ОМС та їхні структурні підрозділи мають широкий спектр повноважень у громаді та реалізують їх різноманітними способами. Це означає, що для запобігання неправомірній обробці та несанкціонованому доступу до персональних даних повинен застосовуватися комплекс заходів.

До основних організаційних заходів можна віднести такі:

1. аналіз діяльності та оцінювання ризиків у сфері обробки персональних даних;
2. організація процесу обробки даних — процедури збору, накопичення, зберігання, передачі, поширення та видалення даних;
3. розробка організаційно-розпорядчих документів;
4. призначення відповідальної особи (структурного підрозділу) за обробку персональних даних і визначення її функціональних обов'язків;
5. розробка правил внутрішнього контролю;
6. упорядкування діяльності щодо передачі даних третім особам.

Питання налагодження всередині ОМС процедур, які б забезпечували якісні процеси накопичення, зберігання та обробки персональних даних, було актуальним і до повномасштабної війни. На практиці досить невелика кількість ОМС мала розроблені та запроваджені внутрішні розпорядчі документи в цій сфері, що своєю чергою призводило до безсистемності та низької ефективності зусиль у реалізації права на захист персональних даних. Навіть у тих ОМС, які мали ухвалені внутрішні розпорядчі документи з питань захисту персональних даних, вони часто були просто скопійовані з інших організацій й не відображали реальних процесів взаємодії між окремими структурними підрозділами органу.

Після початку повномасштабної війни актуальність проблеми зросла — у критичний момент і під загрозою окупації працівники ОМС не мали чіткого розуміння та алгоритму дій, спрямованих на убезпечення витоку персональних даних і перешкоджання їх потраплянню в руки окупантів.

Звичайно, спектр усіх наявних заходів з убезпечення інформації доволі широкий. У цьому матеріалі зупинимося лише на тих, які викликали найбільше питань у працівників ОМС під час спільних дискусій.

1. Що означає проєктування дизайну приватності?

Законодавство у сфері захисту персональних даних вимагає від усіх суб'єктів, які збирають інформацію, спроєктувати належну систему її захисту. Коли мова заходить про організаційні та технічні заходи безпеки даних, то практично завжди згадують два терміни — privacy by design і privacy by default.

Privacy by design
(конфіденційність за допомогою дизайну)
означає, що особа, яка збирає дані, зобов'язана вбудувати систему їх захисту ще на ранньому етапі проєктування й повинна підтримувати таку систему безперервно й надалі. По суті в законі робиться акцент на превенції всіх можливих ризиків, наприклад витоку даних. Погодьтеся, будь-яку проблему завжди краще спрогнозувати й запобігти, ніж потім підраховувати завдану нею шкоду й усувати наслідки.

Privacy by default
(конфіденційність за замовчуванням)
означає, що особам, чиї дані обробляються, не потрібно вживати жодних дій для захисту своєї конфіденційності, бо це має бути забезпечено за замовчуванням. Тобто в діяльність організацій повинні бути впроваджені відповідні технічні та організаційні заходи безпеки інформації. Тут доречно згадати принцип мінімізації даних — що менше даних організація обробляє, то менший ризик порушення закону.

Терміни *privacy by design* і *privacy by default* розроблені ще в 1990-х роках Енн Кавукян, екскомісаркою з питань інформації та конфіденційності провінції Онтаріо (Канада). У 2009 році вона опублікувала документ «Вбудована конфіденційність: сім основних принципів»[9], у якому пояснила, що «вбудована конфіденційність» означає, що компанії повинні активно розглядати питання захисту даних протягом усього циклу їх обробки (full lifecycle protection) — від збору до видалення. Принципи privacy by design і privacy by default ухвалені більшістю країн як стандарт у сфері захисту даних. Підхід «конфіденційність за допомогою дизайну» використовується скоріше для запобігання ризикам, а не усунення наслідків. Люди не повинні доводити своє право на недоторканність приватного життя, воно повинно захищатися за замовчуванням[10].

9 Ann Cavoukian «Privacy by Design. The 7 Foundational Principles». Режим доступу: https://www.ipc.on.ca/wpcontent/uploads/resources/7foundationalprinciples.pdf

10 Уляна Шадська «Аналіз ризиків під час обробки персональних даних: що важливо знати?»

2. Як аналізувати діяльність у сфері обробки персональних даних?

Обробка даних повинна ґрунтуватися на підході, який передбачає систематичний аналіз діяльності в цій сфері та ризиків, які можуть виникнути для осіб, кому вони належать[11]. Тому потрібно періодично описувати всі процеси роботи з даними. Тільки після аналізу того, як функціонує інформація, від збору до видалення, можна зрозуміти проблеми й мінімізувати негативні наслідки.

Така практика має бути не разовою формальністю, а інтегрованим процесом у діяльності установи. Нагадаємо, що обробка — це все те, що відбувається з персональними даними. Тому першим і необхідним етапом є визначення та опис того, на якій підставі, як і чому збирається конфіденційна інформація, кому передається та як це все регулюється.

№	Питання для аналізу діяльності	Результат аналізу
1.	Яка сфера діяльності, завдання та повноваження установи в контексті обробки персональних даних?	*Загальна мета збору персональних даних, відповідно до повноважень конкретного структурного підрозділу (або відділу) ОМС*
2.	Яка правова основа для збору / обробки даних?	*Нормативно-правові акти, що регулюють обробку персональних даних*
3.	Які цілі збору / обробки даних?	*Опис усіх цілей, оскільки їх може бути декілька.*
4.	Які види та категорії даних збираються?	*Перелік видів та категорій даних*
5.	З яких джерел збирається інформація?	*Перелік усіх можливих джерел збору персональних даних*
6.	Які категорії осіб, чиї дані збираються?	*Конкретні цільові групи*

Див. продовження таблиці на наступній сторінці

11 Наприклад, у Регламенті Європейського Парламенту і Ради (ЄС) (GDPR) проведення DPIA є юридичною вимогою для будь-якого типу обробки даних. Особливо вона стосується високого ризику для прав і свобод людини.

№	Питання для аналізу діяльності	Результат аналізу
7.	Які процеси передбачають обробку персональних даних?	*Наприклад, реєстрація, накопичення, поширення, передача тощо. Необхідно описати всі ці процеси та оцінити на відповідність закону*
8.	Яка форма обробки персональних даних?	*Паперова, автоматизована або змішана*
9.	Перелік осіб, що беруть участь в обробці даних і мають доступ до них	П.І.Б. осіб, які мають доступ до баз даних та працюють з ними
10.	Яким чином забезпечуються права суб'єктів персональних даних?	*Відповідно до статті 8 Закону про захист персональних даних*
11.	Відповідальна особа за обробку даних	*Повноваження, сфера відповідальності та напрями роботи (звіти)*
12.	Де зберігається та накопичується інформація?	*Інформаційні ресурси та їх локалізація*
13.	Які терміни зберігання інформації?	*Визначення строків і нормативних актів, що регулюють порядок зберігання даних*
14.	Який порядок доступу до даних з боку третіх осіб?	*Наявність відповідних правил чи інструкцій щодо процедур передачі даних*
15.	Які внутрішні розпорядчі документи регулюють процес обробки даних?	*Перелік положень, інструкцій, наказів та інших правил*
16.	Який порядок видалення інформації?	*Строки та нормативні акти, що регулюють порядок видалення даних*

Відповіді на ці питання дадуть змогу зробити базовий аналіз діяльності установи (або її структурного підрозділу), визначити основні проблеми та загальну стратегію роботи з даними. По суті це інвентаризація всіх процесів обробки інформації, необхідна для узгодження діяльності з вимогами закону.

На підставі аналізу можна визначити приблизний перелік процесів, у межах яких здійснюється обробка даних, що будуть коригуватися залежно від специфіки діяльності установи та її організаційно-правової форми.

Аналіз можна проводити шляхом опитування або інтерв'ю з особами, які здійснюють обробку даних.

Варто також звернути увагу на вимоги нормативних документів, які регулюють інші, ніж захист персональних даних, відносини. Так, наприклад, постанова Кабінету Міністрів України *«Про затвердження Положення про набори даних, які підлягають оприлюдненню у формі відкритих даних»* від 21 жовтня 2015 року № 835 (з наступними змінами)[12] передбачає обов'язок кожного розпорядника інформації, включно з ОМС, проводити інформаційний аудит. Під цим терміном постанова передбачає процес аналізу наявності, стану, форматів, процесів використання всієї інформації. Проведення інформаційного аудиту обов'язкове та має здійснюватися щонайменше один раз на рік.

3. Для чого потрібен реєстр обробки персональних даних?

Реєстр обробки персональних даних — це документ, у якому міститься інформація, як в установі обробляються персональні дані[13]. Наприклад, коли буде відбуватися перевірка з боку контролюючих органів, вони обов'язково запитають про реєстр.

Іншими словами, повертаючись до прикладу з шафою, реєстр має вигляд поличок, на які потрібно розкласти інформацію про обробку. Це легко зробити, коли вже попередньо був проведений аналіз діяльності *(дивіться пункт 2).*

Обов'язкові компоненти реєстру:

1. контактна інформація установи та відповідальної особи з питань захисту персональних даних;
2. правові підстави та джерела збору даних;
3. цілі обробки персональних даних;
4. опис категорій суб'єктів даних і категорій персональних даних;
5. список одержувачів, яким було або буде розкрито дані, включаючи треті країни або міжнародні організації;

12 Постанова Кабінету Міністрів України «Про затвердження Положення про набори даних, які підлягають оприлюдненню у формі відкритих даних». Режим доступу: https://zakon.rada.gov.ua/laws/show/835-2015-%D0%BF#Text

13 У європейському законодавстві, а саме в статті 30 GDPR, встановлено обов'язок вести такий реєстр для кожного контролера та процесора.

6. строки зберігання та видалення даних;
7. відомості про транскордонну передачу персональних даних, якщо така здійснюється;
8. загальний опис технічних й організаційних заходів безпеки.

Найчастіше документ має форму таблиці, кожен рядок якої відповідає певному етапу (виду) обробки, а стовпець — категорії відомостей, які потрібно вказувати в реєстрі. Також обов'язково потрібно зазначити, який саме підрозділ контролює відповідну обробку. Отже, основна мета реєстру — упорядкувати весь цикл обробки персональних даних.

Для ОМС ведення реєстру — необхідна процедура з декількох причин:

— обробка, яку вони здійснюють, з великою ймовірністю може призвести до ризику порушення прав і свобод людини;
— обробка включає особливі категорії даних.

Наявність реєстру в ОМС вказує, що в установі існує контроль за обробкою персональних даних, адже він дозволяє наочно бачити й оцінювати стан справ у цій сфері діяльності органу. Завдяки реєстру можна швидко перевірити або оновити необхідну інформацію, наприклад проконтролювати терміни зберігання та здійснити перевірку на наявність надлишкових даних. Одним словом, у реєстрі всі необхідні відомості зібрані в одному місці, а тому його наявність є однією з умов належного обігу даних в ОМС.

4. Чому потрібно оцінювати ризики у сфері обробки даних?

Управління ризиками[14] полягає у вивченні всіх процесів роботи з даними всередині й ззовні ОМС (у випадках, якщо дані передаються третім особам). Зокрема, ідеться про пошук найбільш вразливих місць у системі захисту інформації, які можуть призвести до витоку, викривлення чи неконтрольованого знищення даних.

Часто виникають питання, чи потрібно кожному структурному підрозділу ОМС окремо проводити оцінювання ризиків, чи це має бути єдина загальна процедура для всіх напрямів роботи.

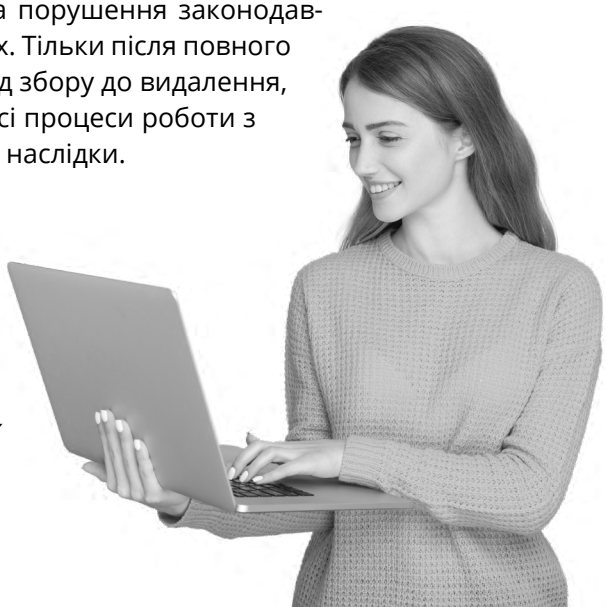
14 У європейському законодавстві оцінювання впливу на захист персональних даних, або Data Protection Impact Assessment (далі — DPIA), — це процедура, передбачена статтею 35 GDPR, а також іншими документами, які визначають міжнародні стандарти безпеки даних.

По-перше, ОМС у різних областях відрізняються за своїм складом. По-друге, з огляду на різноманітність напрямів роботи установи кожен структурний підрозділ збирає окремий вид і категорію персональних даних. Також треба враховувати, що обробка може відбуватися для різних цілей. Це означає, що процедуру оцінювання ризиків краще здійснювати окремо для кожного управління чи департаменту. Водночас хорошою буде вважатися практика, коли в ОМС затверджений єдиний стандарт реалізації цього процесу.

У більшості випадків процес оцінювання ризиків **складається з таких етапів:**

1. **Визначення загального контексту діяльності об'єкта аналізу.** Для початку потрібно проаналізувати напрями роботи загалом і зібрати базову інформацію, що допоможе зрозуміти специфіку діяльності підрозділу, які завдання він виконує, цілі, напрями роботи, повноваження, наявність партнерів, існування режимних обмежень тощо. На практиці це ще називають складанням детального профілю суб'єкта оцінювання.
2. **Визначення мети.** Від мети аналізу напряму залежить сценарій і зміст методології, скільки часу й ресурсів необхідно для його проведення і яким є очікуваний результат.
3. **Складання методології.** Саме від «профілю суб'єкта» буде залежати зміст методології.
4. **Аналіз.** Коли вже є детальний профіль суб'єкта, визначена ціль складена методологія аналізу, настає важливий етап — оцінювання ризиків.
5. **Реагування** (усунення недоліків). Після того, як проблеми (ризики) визначені й зрозумілі, варто подумати про стратегію їх розв'язання та відстеження динаміки змін на краще, адже заради них усе й було затіяно.

Аналіз ризиків — важлива частина зобов'язань щодо підзвітності діяльності ОМС, а також реагування на порушення законодавства у сфері захисту персональних даних. Тільки після повного аналізу того, як циркулює інформація від збору до видалення, можна зрозуміти ризики і вибудувати всі процеси роботи з даними так, щоб мінімізувати негативні наслідки.



Необхідність проведення оцінювання ризиків підтверджена досвідом країн розвиненої демократії і навіть закріплена відповідними актами. Наприклад, у *Регламенті Європейського Парламенту і Ради (ЄС) (GDPR) оцінювання впливу на захист персональних даних*

(DPIA) є юридичною вимогою для будь-якого типу обробки даних. Особливо вона стосується тих, що пов'язані з високим ризиком для прав і свобод людини. Оцінювання також гарантує те, що весь персонал, який бере участь у розробці проєктів, дбає про конфіденційність на ранніх етапах і застосовує підхід privacy by design і privacy by default. Невиконання передбачених вимог може призвести до покарання у вигляді великого штрафу.

Ризики бажано оцінювати окремо для кожної операції з обробки даних, звертаючи особливу увагу на ті, під час проведення яких виникає високий рівень загрози для прав і свобод людини. Залишається додати, що весь цей процес потрібно документувати, щоб у разі виникнення спірних ситуацій можна було обґрунтувати доцільність ухвалення тих чи інших рішень і пояснити, на запобігання яких саме ризиків були спрямовані запроваджені заходи[15].

5. Які внутрішні документи необхідні?

Процес обробки персональних даних складається з різних етапів і процедур, які мають врегульовуватися внутрішніми документами. До їх переліку можна віднести такі:

1. політика щодо обробки персональних даних (або політика приватності)[16];
2. правила використання файлів cookie (у разі збору даних за допомогою інтернет-ресурсів);
3. загальна внутрішня інструкція роботи з даними[17];
4. правила розгляду запитів суб'єктів, чиї дані обробляються;
5. правила здійснення внутрішнього контролю за процесами обробки даних;
6. правила роботи зі знеособленими даними;
7. посадові інструкції осіб, відповідальних за організацію обробки даних;
8. типове зобов'язання про нерозголошення персональних даних;
9. правила передачі персональних даних третім особам або їх поширення.

15 Детальніше з методологією оцінювання ризиків можна ознайомитися за посиланням: https://decentralization.gov.ua/uploads/library/file/774/Posibnyk_ocinka-ryzykiv-ZPD.pdf

16 Документ, розроблений володільцем або розпорядником персональних даних, у якому описано весь процес обробки персональних даних.

17 Чіткі внутрішні правила організації та забезпечення всього циклу обробки даних (збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення тощо).

Цей перелік не є вичерпним, оскільки остаточний зміст пакета необхідної службової документації залежить від специфіки діяльності та повноважень органу, набору функцій інформаційних систем, кількості залученого до роботи з даними персоналу тощо. Головні принципи та правила роботи з персональними даними визначені в політиці обробки персональних даних (або політиці приватності).

Слід зазначити, що чинне законодавство не встановлює прямий обов'язок ухвалювати вказані вище документи, але після ухвалення нового закону про захист персональних даних відповідна вимога може з'явитися. Водночас ретельно продумані, розроблені під потреби кожного ОМС акти внутрішнього користування допоможуть ефективно організувати процеси та повною мірою виконати вимоги закону в цій сфері. Тоді як скопійовані зі стороннього зразка документи аж ніяк не покращать ситуацію.

Під час розробки та затвердження внутрішніх нормативних актів варто пам'ятати, що їх положення не повинні суперечити вимогам законодавства України або допускати довільні тлумачення, які звужують права людини. Також необхідно простежити, щоб запроваджувані документи узгоджувалися з чинними актами, наприклад регламентами рад і виконавчих комітетів, положеннями про постійні комісії та іншими рішеннями. У разі потреби доцільно одночасно з підготовкою нових вносити зміни до чинних актів, щоб уникнути плутанини та нормативних колізій.

6. Що має містити політика приватності?

Уповноважений Верховної Ради України з прав людини опублікував роз'яснення[18], що має містити політика приватності (або політика обробки персональних даних).

Загальні положення:

- законна підстава та мета обробки даних;
- обсяг і категорії даних у співвідношенні з конкретними цілями їх обробки;
- основні принципи, якими керується володілець та уповноважені ним особи під час обробки даних.

18 Рекомендації Уповноваженого Верховної Ради України з прав людини щодо дотримання права на приватність під час встановлення і використання систем відеоспостереження у громадських місцях. Режим доступу: https://ombudsman.gov.ua/storage/app/media/ЗПД/Рекомендації%20щодо%20дотримання%20права%20на%20приватність.pdf

Права суб'єкта персональних даних:

- право на інформування;
- право на доступ до своїх персональних даних;
- право на виправлення та видалення своїх персональних даних;
- право на заперечення проти обробки своїх персональних даних;
- процедура розгляду запитів та оскарження.

Процедури обробки персональних даних:

- інформаційні системи, програмне забезпечення, сервери, задіяні в процесі обробки персональних даних;
- перелік організаційних і технічних заходів безпеки;
- строк зберігання та порядок видалення інформації.

Обробка даних, що здійснюється розпорядниками:

- загальні положення про умови та мету передачі персональних даних;
- правила виконання вимог щодо захисту персональних даних;
- заходи в разі припинення договірних відносин.

Передача персональних даних третім особам:

- процедури та правила передачі персональних даних третім особам;
- порядок здійснення контролю.

Внутрішній контроль:

- особа, відповідальна за безпеку персональних даних;
- порядок надання права доступу працівників до персональних даних;
- проведення внутрішніх перевірок щодо дотримання правил безпеки при обробці персональних даних.

Цю структуру можна взяти за основу для складання власної політики приватності. З метою забезпечення принципів прозорості й підзвітності суспільству документи, які регламентують обробку персональних даних, мають бути у вільному доступі (наприклад, на офіційному вебсайті ОМС).

У документі також треба вказати контактні дані, куди запитувач може подати запит на персональні дані, і графік роботи, коли зацікавлені особи можуть ознайомитися з документами, отримати консультацію тощо. Також потрібно забезпечити механізм розгляду запитів про доступ до персональних даних і надання довідкової інформації.

В ОМС можуть бути власні підходи до організації обробки даних і налагодження взаємодії окремих посадових осіб чи структурних підрозділів у процесі підготовки відповідей на запити суб'єктів персональних даних або третіх осіб. Тож у цій частині політики приватності варто зазначити:

— повноваження з ухвалення рішення про надання даних чи відмову;
— повноваження з підписання відповідей (передача права підпису відповідальній особі, яка готує відповідь, сприятиме скороченню строків підготовки відповідей і якнайшвидшому розгляду й задоволенню запитів);
— алгоритм обліку запитів суб'єктів персональних даних чи третіх осіб.

7. Який обсяг даних можна збирати?

Персональні дані не можуть колекціонуватися чи збиратися «про всяк випадок». Вони є інструментом досягнення конкретної й заздалегідь визначеної мети, а отже, повинні оброблятися тільки в тих випадках, коли в інший спосіб досягти цієї мети неможливо або обробка даних дозволена законом. Якщо це не зашкодить виконанню поставлених завдань, потрібно використовувати анонімні дані. Там, де необхідні лише персональні дані, вони повинні бути адекватними, актуальними й містити мінімум інформації, який забезпечує отримання очікуваного результату (*міжнародний принцип «мінімізації даних» або «пропорційності»).*

Для того, щоб на практиці застосувати принцип пропорційності, потрібно відповісти на такі питання: *які дані, у якому форматі і у який спосіб потрібно збирати для досягнення поставленої мети?*

Наприклад, система відеонагляду буде зайвою для того, щоб виявляти факти тютюнопаління в адміністративній будівлі ОМС, — для цього достатньо встановити чутливі датчики диму, які водночас забезпечать протипожежний і захист від інших загроз. Або не завжди при вході в будівлю

потрібно здійснювати аудіо- та відеоспостереження. Доцільність використання тих чи інших функцій техніки має бути обґрунтована. Те саме стосується й запиту ОМС для отримання даних у зверненнях громадян.

У документах ОМС з метою надання муніципальних послуг може бути вимога щодо збору спеціальної категорії даних особи: про расове, етнічне та національне походження, релігійні та світоглядні переконання. Якщо ця інформація не є вкрай необхідною для реалізації конкретної функції, вона однозначно буде надлишковою.

8. Навіщо призначати відповідальну особу?[19]

Питання швидше риторичне. Якщо законодавство встановлює відповідальність за порушення правил роботи з персональними даними, то має бути й особа, яка буде таку відповідальність нести.

Стаття 24 Закону України *«Про захист персональних даних»* передбачає, що в ОМС, а також у володільців чи розпорядників персональних даних, що здійснюють їх обробку, створюється (визначається) структурний підрозділ або відповідальна особа, яка організовує роботу, пов'язану із захистом даних при їх обробці. Зауважимо, що закон не висуває конкретних вимог до посади та рівня освіти відповідальних осіб, а лише вказує, що вони:

1. інформують і консультують володільця або розпорядника персональних даних з питань додержання законодавства про захист персональних даних;
2. взаємодіють з Уповноваженим Верховної Ради України з прав людини та визначеними ним посадовими особами його секретаріату з питань запобігання й усунення порушень законодавства про захист даних.

Це означає, що установа (або структурний підрозділ) ухвалює рішення про обов'язки відповідальної особи на власний розсуд, проте з урахуванням таких аспектів:

1. уникнення конфлікту інтересів — особа має підпорядковуватися безпосередньо керівнику установи;
2. особа повинна мати достатньо повноважень для виконання покладених на неї функцій.

19 Станом на момент підготовки цього документа нова редакція Закону України «Про захист персональних даних» ще була на розгляді Верховної Ради України. Розроблений законопроєкт передбачає запровадження в установах, підприємствах та організаціях, у тому числі ОМС, спеціальної посади для особи, відповідальної за захист персональних даних. Таке положення узгоджує правила національного законодавства з вимогами міжнародних документів у цій сфері.

Призначення відповідальної особи необхідно оформити наказом, з яким вона ознайомлюється під підпис. Звісно, що в ОМС, які не мають достатнього бюджету на окрему штатну одиницю, такі обов'язки можуть бути покладені на когось з працівників виконавчого комітету ради. У будь-якому випадку весь спектр обов'язків має бути детально описаний у посадовій інструкції.

Як показали перші місяці повномасштабної війни, переважна частина ОМС жодним чином не врегулювали у своїх розпорядчих документах алгоритм дій щодо матеріальних носіїв з базами персональних даних у воєнний час або перед загрозою окупації. Так, наприклад, у ОМС ведуться журнали обліку звернень громадян, прийому громадян, у яких фіксуються такі персональні дані, як ПІБ та адреса, а також часто дані про предмет звернення чи особливий статус заявника. Також відповідно до Закону України *«Про місцеве самоврядування в Україні»* до відання виконавчих рад віднесені делеговані повноваження у сфері реєстрації місця проживання фізичних осіб і ведення реєстру територіальної громади. Здійснюючи зазначені повноваження, виконавчі комітети ОМС накопичували значну кількість персональних даних осіб, зареєстрованих на території відповідної адміністративно-територіальної одиниці.

Окрім того, у відділах кадрів, відділах діловодства та архівних відділах виконавчих комітетів ОМС зберігалися великі обсяги персональних даних працівників ОМС і депутатів місцевих рад, особові справи яких містили, зокрема, автобіографії, фотографії, відомості про склад сім'ї тощо. У значної кількості ОМС такі матеріальні носії зберігалися в кабінетах відповідних працівників, приймальнях керівників, відділах діловодства тощо.

На початку повномасштабної збройної агресії відповідальні працівники не були проінструктовані про необхідність вивозу в безпечне місце або знищення баз персональних даних, витоки яких могли зашкодити життю та безпеці мешканців громади. Подібна недбалість і розгубленість (а подекуди й злочинний умисел) призвели до того, що на окремих тимчасово окупованих територіях накопичені в ОМС масиви персональних даних потрапили до загарбників і наразі використовуються ними у своїх цілях.

З метою кращої організації виконання всіх вимог інформаційного законодавства доцільно поєднувати обов'язки особи, відповідальної за захист персональних даних, та особи, відповідальної за доступ до публічної інформації. Така оптимізація сфер відповідальності зумовлена тим, що питання виконання вимог Закону України *«Про захист персональних даних»* і

Закону України *«Про доступ до публічної інформації»* часто перетинаються як у частині обробки запитів, так і фахової підготовки.

Досить поширеною проблемою при організації захисту даних є дроблення ОМС на окремих юридичних осіб, на кожну з яких покладається весь комплекс обов'язків і повноважень. Однак людина може не знати, що окремі департаменти чи управління — це окремі юридичні особи, а отже, окремі володільці даних. Як правило, люди звертаються на загальну адресу ради для з'ясування того, який саме відділ повинен їм відповідати, що породжує зайвий документообіг і призводить до нераціонального використання ресурсів органу та робочого часу.

Тож важливо, щоб внутрішні документи, які розроблюються виконавчим комітетом ОМС, містили його реальну структуру (враховували всі підпорядковані підрозділи) та могли забезпечити оптимальні шляхи виконання вимог законодавства про захист персональних даних без бюрократичної тяганини. З огляду на це рекомендуємо місцевим радам розробити й ухвалити окремий розпорядчий документ «*Про організацію роботи ради та її виконавчих органів щодо забезпечення захисту персональних даних*», у якому врегулювати такі питання:

a. створення структурного підрозділу або визначення відповідальної особи за координацію роботи ради та її виконавчих органів щодо захисту персональних даних з такими повноваженнями:
   - — контролювати виконання вимог Закону України «Про захист персональних даних» апаратом ради та її виконавчим комітетом, іншими виконавчими органами;
   - — видавати обов'язкові для виконання службовцями цих органів рішення про усунення порушень законодавства про захист персональних даних;
   - — консультувати службовців ОМС, працівників комунальних підприємств, бюджетних установ, комунальних закладів, органів самоорганізації населення територіальної громади щодо особливостей виконання законодавства у сфері персональних даних;
   - — організовувати відповідні навчання та підвищення кваліфікації;

b. призначення відповідальних осіб для забезпечення захисту персональних даних в апараті ради, її виконавчому комітеті та виконавчих органах. Тобто визначити перелік посад, за якими закріпити весь спектр обов'язків з виконання законодавства про захист персональних даних. Відповідальність за їх реалізацію та рівень наданих для цього повноважень мають бути прописані в посадових інструкціях і функціональних обов'язках відповідних працівників.

На жаль, навіть у тих ОМС, де призначені відповідальні особи, їх посадові інструкції замість деталізованого переліку обов'язків містять лише загальні формулювання про забезпечення виконання вимог спеціального законодавства про захист персональних даних. Практично не відомі випадки, коли б посадові інструкції відповідальних осіб чи інші внутрішні розпорядчі документи передбачали реалізацію конкретних заходів з унеможливлення витоків персональних даних, хоча в ситуації загрози окупації території громади такі заходи мають вживатися в першу чергу.

9. Які функціональні обов'язки виконує відповідальна особа?

Відповідальна особа — це не безпосередній виконавець, а здібний організатор, ефективний управлінець й суворий контролер. Ключове завдання відповідальної особи — розроблення стратегії обробки й захисту даних і систематичний контроль за її реалізацією.

До функціональних обов'язків відповідальної особи доцільно віднести такі:

- контроль за проведенням заходів із захисту персональних даних;
- ведення обліку процесів обробки даних;
- розробка та підтримання в ктуальному стані відповідної внутрішньої документації;
- здійснення оцінювання ризиків і забезпечення внутрішнього контролю за дотриманням законодавства про захист даних;
- підвищення кваліфікації персоналу з питань захисту персональних даних;
- організація прийому та розгляд звернень (запитів) суб'єктів персональних даних, а також запитів третіх осіб;
- організація службових перевірок за фактами порушень вимог до обробки й захисту персональних даних, а також інших інцидентів інформаційної безпеки;
- підготовка органу до перевірок з боку контролюючих інстанцій й організаційне сприяння їх якісному проведенню (розробка необхідних документів, надання затребуваної інформації, налагодження комунікації тощо);

— взаємодія з Уповноваженим Верховної Ради України з прав людини, іншими державними органами контролю та неурядовими громадськими організаціями з питань забезпечення прав, свобод і законних інтересів громадян під час обробки персональних даних;

— дослідження всіх аспектів діяльності, пов'язаних із захистом персональних даних (зміни в законодавстві, інновації, технології тощо)[20].

Наприклад, часто на практиці особи, яких призначили відповідальними за роботу з персональними даними, є фахівцями з правовідносин у цій сфері, але їм складно контролювати технічну складову — процес обробки даних за допомогою інформаційних систем і технологій (вебсайт, системи відеоспостереження тощо). Тому відповідальна особа, окрім юридичних, повинна володіти специфічними технічними знаннями або налагодити співпрацю з IT-спеціалістами.

Особливо важливо забезпечити належний рівень підготовки працівників, що опікуються захистом персональних даних у воєнний час, адже помилки та недоліки в роботі в цей період можуть мати тяжкі наслідки.

Зрозуміло, що й керівники органу свою участь у роботі із захисту персональних даних не повинні обмежувати лише підписанням наказу про призначення відповідальної особи, адже запорукою успішності будь-якого кадрового рішення є виважений відбір кандидата на посаду й створення належних умов для продуктивної праці. Тому перед призначенням керівник має відповісти собі на такі питання:

— Чи є у відповідальних осіб точні та актуальні посадові інструкції?

— Чи усвідомлюють призначені особи важливість покладених на них обов'язків та чи знають, як їх треба виконувати на практиці?

— Чи достатньо в них ресурсів і повноважень для виконання доручених завдань?

20 Наведений перелік обов'язків не є вичерпним. У кожному окремому випадку необхідно визначити обсяг повноважень, що дозволяє гарантувати належну обробку та захист даних.

10. Який порядок доступу до даних з боку третіх осіб?

Спочатку визначимося з термінологією. «Третьою особою» вважається будь-яка особа, за винятком суб'єкта, володільця чи розпорядника персональних даних та Уповноваженого Верховної Ради України з прав людини.

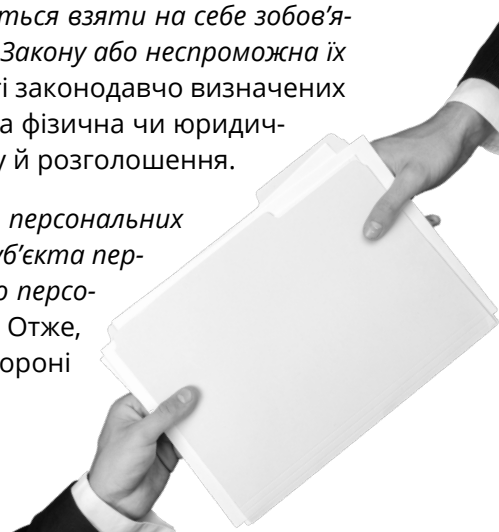
Передача персональних даних третім особам — це один з видів обробки даних, у результаті якого доступ до інформації про людину, окрім володільця й розпорядника даних, отримує ще хтось, наприклад правоохоронець або журналіст. Зрозуміло, що іноді це може призвести до обурення цієї людини, звинувачень з її боку, судових позовів тощо. Тому доступ третіх осіб до персональних даних має відбуватися відповідно до правових норм без жодних винятків.

Для ухвалення рішення про можливість передачі персональних даних третім особам насамперед слід з'ясувати наміри щодо їх подальшого використання. Це необхідно, оскільки процедура надання третім особам доступу до даних здійснюється володільцем не на власний розсуд, а лише у визначений законодавством спосіб і за наявності відповідних правових підстав.

У статті 19 Конституції України визначено, що правовий порядок у державі ґрунтується на засадах, відповідно до яких ніхто не може бути примушений робити те, що не передбачено законодавством. Органи державної влади та їх посадові особи зобов'язані діяти лише на підставі, у межах повноважень та у спосіб, що передбачені Конституцією та законами України. З огляду на це надавати інформацію на запит можна лише за наявності повноважень, законної підстави, обґрунтованої мети та в спосіб, передбачений законом.

Тепер про головне: обов'язок забезпечити належний захист персональних даних у випадку їх поширення чи передачі покладається на сторону, яка їх поширює чи передає. Водночас стаття 16 Закону України *«Про захист персональних даних»* наголошує: *«доступ до персональних даних третій особі не надається, якщо зазначена особа відмовляється взяти на себе зобов'язання щодо забезпечення виконання вимог цього Закону або неспроможна їх забезпечити»*. Одним словом, навіть за наявності законодавчо визначених підстав персональні дані може отримати лише та фізична чи юридична особа, яка зможе і буде їх захищати від витоку й розголошення.

Ця ж стаття вказує, що *«порядок доступу до персональних даних третіх осіб визначається умовами згоди суб'єкта персональних даних на їх обробку, надану володільцю персональних даних, або відповідно до вимог закону»*. Отже, передача персональних даних людини третій стороні



є законною, якщо людина заздалегідь знала про таку можливість і дала на це відповідну згоду. Винятки з цього правила можливі тільки у визначених законом випадках і лише в інтересах національної безпеки, захисту економічного добробуту та прав людини.

Передача даних третім особам здійснюється на підставі офіційного запиту, у якому мають бути зазначені:

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

Строк вивчення запиту не може перевищувати *десяти робочих днів* з дня надходження. Протягом цього строку необхідно повідомити особу, яка подала запит, чи буде його задоволено або чому запитувана інформація не підлягає наданню. Запит розглядається протягом *тридцяти* календарних днів з дня надходження, якщо інше не передбачено законом.

Наприклад, порядок передачі персональних даних органам правопорядку роз'яснений у листі Представника Уповноваженого Верховної Ради України з прав людини від 28 грудня 2015 року «*Щодо правових підстав передачі персональних даних правоохоронним органам*»[21], у якому вказується, що «*належною підставою для отримання правоохоронними органами доступу до даних в рамках кримінального провадження є ухвала слідчого судді, суду про тимчасовий доступ до речей і документів. Усі інші запити на доступ до персональних даних мають розглядатися індивідуально з огляду на повноваження запитувача, підстави запиту, обсяг запитуваної інформації тощо».*

21 Офіційний сайт Уповноваженого Верховної Ради України з прав людини. Режим доступу: https://ombudsman.gov.ua/ua/publication/petition/schodo-pravovix-pidstavperedachipersonalnix-danix-pravooxoronnim-organam/

Як уже зазначено вище, до окремої категорії персональних даних доступ не повинен обмежуватися. Ідеться насамперед про дані, визначені статтею 5 Закону України «Про захист персональних даних»:

— персональні дані, що стосуються здійснення особою, уповноваженою на виконання функцій держави або місцевого самоврядування, посадових або службових повноважень;

— персональні дані, зазначені в декларації особи, уповноваженої на виконання функцій держави або місцевого самоврядування, оформленій за формою, визначеною відповідно до Закону України «Про запобігання корупції», окрім відомостей, визначених Законом України «Про запобігання корупції»;

— інформація про отримання в будь-якій формі фізичною особою бюджетних коштів, державного чи комунального майна, структуру, принципи формування та розмір оплати праці, винагороди, додаткового блага керівника, заступника керівника юридичної особи публічного права, керівника, заступника керівника, члена наглядової ради державного чи комунального підприємства або державної чи комунальної організації, що має на меті одержання прибутку, особи, яка постійно або тимчасово обіймає посаду члена виконавчого органу чи входить до складу наглядової ради господарського товариства, у статутному капіталі якого більше як 50 % акцій (часток, паїв) прямо чи опосередковано належать державі та/або територіальній громаді, окрім випадків, передбачених статтею 6 Закону України «Про доступ до публічної інформації»;

— інформація про фізичних осіб, які мають податковий борг, що публікується на офіційному вебпорталі центрального органу виконавчої влади, який реалізує державну податкову політику, відповідно до вимог пункту 35.4 статті 35 Податкового кодексу України;

— інші відомості, що є персональними даними, щодо яких заборонене законом віднесення до інформації з обмеженим доступом.

На практиці в багатьох ОМС виникають складнощі, коли до них надходить інформаційний запит, відповідь на який потребує надання персональних даних третіх осіб. Закон України *«Про захист персональних даних»*[22] *передбачає вимоги до оформлення запиту на персональні дані, які не збігаються з вимогами до запиту на інформацію відповідно до Закону України «Про доступ до публічної інформації»*[23].

22 Стаття 16 Закону України «Про захист персональних даних».

23 Стаття 19 Закону України «Про доступ до публічної інформації».

Так, фізична особа, яка подає запит у порядку, передбаченому Законом України *«Про захист персональних даних»*, повинна вказати своє прізвище, ім'я та по батькові, місце проживання і реквізити документа. Водночас інформаційний запит, поданий за правилами законодавства про доступ до публічної інформації, не повинен містити інформації про місце проживання запитувача та реквізити його документів. Іншими словами, для належного подання запиту на персональні дані важливо ідентифікувати особу запитувача, натомість для інформаційного запиту така вимога не є обов'язковою. Навіть більше — законодавство про доступ до публічної інформації передбачає можливість подання анонімних запитів.

Розібратися допоможуть положення законодавства про захист персональних даних, які роз'яснюють, що порядок доступу третіх осіб до персональних даних, якими володіє розпорядник публічної інформації, визначається Законом України *«Про доступ до публічної інформації»*. Коли йдеться про ОМС, уся інформація, яка перебуває у їх розпорядженні, публічна, а отже, обмежувати доступ до неї слід за правилами відповідного закону. Обмеження доступу до інформації, що перебуває у розпорядженні ОМС, здійснюється тільки за результатом застосування частини 2 статті 6 Закону України *«Про доступ до публічної інформації»* (так званого трискладового тесту). Відповідно до цієї правової норми обмеження можливе при дотриманні сукупності таких вимог:

— лише в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету й неупередженості правосуддя;
— розголошення інформації може завдати істотної шкоди цим інтересам;
— шкода від оприлюднення такої інформації переважає суспільний інтерес у її отриманні.

Більш детальна інформація про застосування трискладового тесту міститься в пункті 6 постанови Пленуму Вищого адміністративного суду України від 29 вересня 2016 року № 10 *«Про практику застосування адміністративними судами законодавства про доступ до публічної інформації»*, де наведені категорії конфіденційної інформації, які не можуть бути обмежені в доступі, і зазначений перелік обставин, які повинні враховуватися при розв'язанні питання про обмеження доступу до інформації через її віднесення до конфіденційної.

Ще раз наголосимо, що питання визначення балансу прав та інтересів при розв'язанні питання про надання доступу до інформації віднесене на розсуд відповідальних працівників ОМС. Застосування обмеження на доступ до інформації — відповідальне рішення, яке потребує від працівника ґрунтовних знань і постійного підвищення рівня кваліфікації. Значення таких рішень особливо зростає у воєнний час. Тому ми ще раз рекомендуємо керівникам ОМС визначити працівника, відповідального за захист персональних даних (також ця особа може відповідати і за доступ до публічної інформації), і забезпечити йому можливості для навчання.

Коли йдеться про персональні дані працівника ОМС, члена виконавчого комітету або депутата ради, слід пам'ятати, що доступ до них не завжди може бути обмежений на бажання такої особи. Інформація, яка стосується коштів або майна, отриманих такою особою з місцевого бюджету, не може бути обмежена в доступі. Також у відповідь на запит слід надавати інформацію, яка стосується компетентності та належного виконання такою особою своїх обов'язків, наприклад інформацію про освіту, трудовий стаж, відвідування сесій тощо.

При розв'язанні питання про обмеження доступу до інформації володілець повинен діяти добросовісно, надавати вичерпну відповідь на всі питання запиту, застосовувати обмеження до окремих категорій інформації, а не до всього документа, і позначати в документі місця, де інформація була вилучена. Такий обов'язок запроваджує нещодавно ратифікована Україною *Конвенція Ради Європи про доступ до офіційних документів*. Інформація з обмеженим доступом також має надаватися розпорядником інформації, якщо він правомірно оприлюднив її раніше.

Так само при поширенні персональних даних слід пам'ятати про те, що окремі їх категорії не можуть бути обмежені в доступі — на цьому наголошують приписи законів. Так, наприклад, відповідно до частини 2 статті 5 Закону України *«Про захист персональних даних»* не є конфіденційною інформацією персональні дані, що стосуються здійснення особою, уповноваженою на виконання функцій держави або місцевого самоврядування, посадових або службових повноважень.

11. Який порядок надання персональних даних у відповідь на адвокатський запит?

Існує окрема категорія запитів, що надходять до суб'єктів владних повноважень, у тому числі ОМС, — адвокатські запити відповідно до Закону України *«Про адвокатуру та адвокатську діяльність»*. Такі запити часто містять прохання надати саме персональні дані, необхідні для правової допомоги клієнту.

Проте адвокатський запит повинен мати не тільки клопотання про надання інформації, а й документи, що підтверджують правові взаємини адвоката та клієнта, який потребує захисту в конкретній справі. Щоб мати право отримати персональні дані у відповідь на адвокатський запит, адвокат повинен додати до запиту:

— копію ордера або доручення органу (установи), уповноваженого законом на надання безоплатної правової допомоги;

— завірену підписом самого адвоката копію свідоцтва про право на заняття адвокатською діяльністю.

Вимагати від адвоката подання разом з адвокатським запитом інших документів заборонено. Відповідно до частини 3 статті 24 Закону України *«Про адвокатуру та адвокатську діяльність»* адвокатський запит не може стосуватися надання консультацій і роз'яснень положень закону. Тобто якщо адвокатові чи пересічному громадянинові необхідно отримати інформацію про ситуацію, яка стосується прав і законних інтересів, порушених стосовно саме цього громадянина, їм краще скористатися інструментами, передбаченими Законом України *«Про звернення громадян».*

Відповідальним особам слід пам'ятати, що відповідь на адвокатський запит стосується надання інформації, але не оригіналів документів. Таку позицію викладено в постанові Верховного Суду від 22 липня 2020 року у справі № 299/3792/17, де зазначено:

«53. Аналіз положень статті 24 Закону України «Про адвокатуру та адвокатську діяльність», у якій розкрито зміст і мету адвокатського запиту, у взаємозв'язку з положеннями Законів № 2657-XII, № 2297-VI та № 2939-VI, що визначають режим і порядок доступу до інформації, у тому числі конфіденційної, дають підстави для висновку, що адвокатський запит є способом отримання копій документів, необхідних адвокату для надання правової допомоги клієнту, і не є підставою для вилучення (виїмки) оригіналів рішень органів місцевого самоврядування».

Протиправна відмова в наданні інформації у відповідь на інформаційний і адвокатський запит є адміністративним правопорушенням, передбаченим статтею 212-3 Кодексу України про адміністративні правопорушення.

12. Чи допускається відстрочення доступу третіх осіб до даних?

Сам суб'єкт персональних даних повинен завжди мати безперешкодний доступ до них і відстрочення такого доступу не дозволяється законом. Водночас доступ третіх осіб до даних може бути відстрочений у разі, якщо вони не можуть бути надані протягом 30 календарних днів з дня надходження запиту. При цьому загальний термін розгляду запиту третьої особи на отримання персональних даних не повинен перевищувати *сорока п'яти календарних днів*[24]. Повідомлення про відстрочення доводиться до відома третьої особи, яка подала запит, у письмовій формі з роз'ясненням порядку оскарження такого рішення. У повідомленні про відстрочення зазначаються:

— прізвище, ім'я та по батькові посадової особи;
— дата відправлення повідомлення;
— причина відстрочення;
— строк, протягом якого буде задоволено запит.

Третій особі може бути відмовлено в наданні інформації, якщо доступ до неї прямо заборонений законом. У такому випадку відмова оформлюється повідомленням, у якому зазначаються:

— прізвище, ім'я, по батькові посадової особи, яка відмовляє в доступі;
— дата відправлення повідомлення;
— обґрунтована причина відмови.

Рішення про відстрочення або відмову в доступі до персональних даних може бути оскаржене до Уповноваженого Верховної Ради України з прав людини або суду. Слід узяти до уваги, що відстрочення доступу третіх осіб до персональних даних, передбачене Законом України *«Про захист персональних даних»,* відрізняється від відстрочення доступу до публічної інформації, передбаченого статтею 22 Закону *України «Про доступ до публічної інформації»*. Відповідальним працівникам ОМС варто дотримуватися вимог того із законів, відповідно до якого звернувся запитувач.

Також варто пам'ятати, що Закон України *«Про доступ до публічної інформації»* містить норму, яка передбачає доступ особи до інформації про

24 Стаття 17 Закону України «Про захист персональних даних».

неї[25]. На практиці часто виникає плутанина, правила якого закону слід застосовувати. У цьому випадку відповідальні працівники ОМС повинні послуговуватися принципом доброчесності й докладати зусиль до того, щоб обмеження прав осіб, які звернулися із запитом на інформацію про себе, було мінімальним. Усунення цього недоліку в нормуванні вже включене до планів робочих груп, які розробляють відповідні законопроєкти.

13. Як упорядкувати договірні відносини з розпорядниками?

При передачі персональних даних розпоряднику (за договором) необхідно розробити документ, у якому описати процедури обробки та захисту інформації. Це потрібно для того, щоб обидві сторони (володілець і розпорядник персональних даних) розуміли свої зобов'язання.

Наприклад, що має передбачати такий договір (або інший правовий акт)?

1.	2.
Деталі обробки даних, включаючи:	**Умови передачі або зобов'язання розпорядника після отримання даних, який повинен:**
— характер й мету обробки; — категорії та вид персональних даних; — обов'язки і права володільця даних.	— діяти відповідно до інструкцій володільця даних, за винятком випадків, коли закон вимагає діяти без таких інструкцій; — гарантувати безпеку даних під час їх обробки; — вживати відповідних заходів для забезпечення безпеки обробки; — залучати сторонніх осіб тільки з попереднього дозволу володільця даних і відповідно до договору; — видалити (або повернути) всі персональні дані після завершення дії договору, якщо закон не вимагає їх зберігання.

25 Стаття 10 Закону України «Про доступ до публічної інформації».

14. Яка відповідальність передбачена за порушення законодавства про захист персональних даних?

Контроль за додержанням законодавства в цій сфері здійснюють Уповноважений Верховної Ради України з прав людини та суди[26]. Порушення законодавства про захист даних тягне за собою відповідальність, яка передбачена:

— Кримінальним кодексом України (статтями 182 «Порушення недоторканності приватного життя» і 359 «Незаконні придбання, збут або використання спеціальних технічних засобів отримання інформації»);

— Кодексом України про адміністративні правопорушення (статтею 188-39 «Порушення законодавства у сфері захисту персональних даних»).

Кодекс України про адміністративні правопорушення передбачає покарання у вигляді адміністративного штрафу як за ігнорування вимог Уповноваженого, так і недодержання порядку захисту персональних даних[27].

Контроль за додержанням законодавства про захист персональних даних здійснюється Уповноваженим з прав людини або його представниками шляхом проведення перевірок — планових, позапланових, виїзних і безвиїзних. Як зазначено вище, перевірки можуть проводитися за результатами скарги, що надійшла до Уповноваженого.

У випадку проведення перевірки посадові особи ОМС зобов'язані забезпечити доступ представників Уповноваженого з прав людини до приміщень, матеріалів і документів, необхідних для проведення перевірки, надавати запитувану ними інформацію, пояснення щодо фактичної і правової підстави своїх дій і рішень, а також забезпечити належні умови для проведення перевірки.

26 Відповідно до статті 22 Закону України «Про захист персональних даних».

27 Наказом Уповноваженого Верховної Ради України з прав людини від 8 січня 2014 року № 1/02-14 затверджено Порядок здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних.

15. Які права має суб'єкт персональних даних?

Будь-яка обробка даних — це встановлення певних інформаційно-правових відносин, у яких людина — суб'єкт персональних даних — має безумовні й неоспорювані переваги перед володільцем чи розпорядником. Це цілком логічно й зрозуміло, адже персональні дані є власністю людини та тільки вона має право розпоряджатися ними. Законодавство наголошує, що *«особисті немайнові права на персональні дані, які має кожна фізична особа, є невід'ємними і непорушними».*

Тепер детальніше. Суб'єкт персональних даних має право:

1. Знати про джерела збирання, місцезнаходження своїх персональних даних, мету їх обробки, місцезнаходження (перебування) володільця чи розпорядника даних або дати відповідне доручення щодо отримання цієї інформації уповноваженим ним особам, окрім випадків, встановлених законом.
2. Отримувати інформацію про умови надання доступу до своїх даних, зокрема інформацію про третіх осіб, яким передаються дані (окрім випадків, визначених законом).
3. Мати доступ до своїх даних.
4. Отримувати не пізніше як за тридцять календарних днів з дня надходження запиту, окрім випадків, передбачених законом, відповідь про те, чи обробляються його дані, а також отримувати інформацію про їх зміст.
5. Пред'являти вмотивовану вимогу із запереченням проти обробки своїх даних (окрім випадків, визначених законом).
6. Пред'являти вмотивовану вимогу щодо зміни або знищення своїх даних, якщо ці дані обробляються незаконно чи є недостовірними.
7. На захист своїх персональних даних від незаконної обробки та випадкової втрати, знищення, пошкодження у зв'язку з умисним приховуванням, ненаданням чи несвоєчасним їх наданням, а також на захист від надання відомостей, що є недостовірними чи ганьблять честь, гідність та ділову репутацію фізичної особи.
8. Звертатися зі скаргами на обробку своїх даних до Уповноваженого Верховної Ради України з прав людини або до суду.
9. Застосовувати засоби правового захисту в разі порушення законодавства про захист персональних даних.
10. Вносити застереження стосовно обмеження права на обробку персональних даних під час надання згоди.

11. Відкликати згоду на обробку персональних даних, окрім випадків, коли згода (як правова підстава на збір даних) не застосовується.
12. Знати механізм автоматичної обробки персональних даних.
13. На захист від автоматизованого рішення, яке має для нього правові наслідки[28].

28 Стаття 8 Закону України «Про захист персональних даних».

РОЗДІЛ ІІІ
ЗАХОДИ ДЛЯ БЕЗПЕКИ ДАНИХ

З одного боку, законодавство покладає на ОМС обов'язок захищати персональні дані від незаконної обробки, доступу, випадкової втрати чи знищення, а з іншого — не деталізує правові інструменти та механізми здійснення такого захисту. За цих умов постає завдання розробити власну політику безпеки, яка передбачатиме реалізацію комплексу технічних й організаційних заходів на всіх етапах їх обробки — отримання, накопичення, зберігання, використання, надання третім особам.

Усі ці заходи мають сприяти виконанню першочергових завдань, а саме:

— передбачити організаційно-технічні рішення, які мінімізують несанкціоноване втручання в роботу систем;
— звести до мінімуму ризики порушення законодавства під час роботи з даними;
— забезпечити прозорість їх обробки на всіх етапах;
— надати людині можливість контролювати обробку своїх даних.

1. Що необхідно визначити при розробці заходів із захисту інформації?

При розробці заходів із захисту інформації необхідно визначити:

А. Потенційні загрози для ***персональних даних і можливі джерела їх виникнення***

Існує багато способів незаконно «витягнути» дані з інформаційних систем, серед яких найбільш поширені такі:

— протиправне копіювання даних;
— проникнення в комп'ютери інших користувачів, іноді за допомогою чужих засобів ідентифікації (логінів, паролів, смарткарт);
— використання дефектів програм й операційних систем;
— застосування шкідливих програм;
— нелегітимне підключення до мережі;
— розкрадання носіїв даних;
— фотографування екрана.

Визначення і формулювання загроз дасть можливість:

— провести загальний аналіз захищеності систем;
— здійснити модернізацію систем для мінімізації та (або) нейтралізації встановлених загроз;
— удосконалити методи контролю за захищеністю даних у системах.

Тому важливо завчасно прорахувати ризики залежно від отримуваної інформації та ступеня її конфіденційності, що дозволить запровадити відповідні ризикам заходи безпеки.

B. Об'єкти в інформаційних системах, ***що підлягають захисту***

У першу чергу до таких об'єктів слід віднести:

— персональні дані, що обробляються в інформаційних системах або в паперовому вигляді;
— самі інформаційні ресурси систем (файли, відеоархіви, бази даних тощо);
— обчислювальну техніку та апаратне забезпечення, задіяне в процесах обробки даних;
— програмне (вбудоване, системне) забезпечення, за допомогою якого здійснюється обробка даних;
— документацію, у тому числі технічну, справи чи облікові журнали, картотеки, реєстри, відео-, фото- та інші матеріали, у яких зафіксована чи відображена інформація, що захищається;
— канали (лінії) зв'язку, включаючи кабельні системи;
— мережевий трафік;
— приміщення, у яких здійснюється обробка даних, розміщуються чи зберігаються ресурси інформаційних систем;
— серверне обладнання (операційні системи фізичних серверів, віртуальних серверів, системи управління базами даних тощо), призначене для зберігання даних в інформаційних системах;
— мережеве та телекомунікаційне обладнання тощо.

C. Технічні рішення, необхідні для ***захисту персональних даних,*** порядок і строки їх реалізації

Як правило, такі рішення передбачають:

— проєктування системи захисту, розробку робочої та експлуатаційної документації;
— закупівлю, постачання, встановлення і налаштування технічних, програмних і програмно-технічних засобів захисту інформації;

— проведення дослідницької експлуатації засобів захисту;
— забезпечення технічного захисту приміщень, де проводиться обробка персональних даних (системи сигналізації, відеоспостереження, протипожежного захисту тощо).

D. Заходи ***з нормативного та кадрового врегулювання*** питань інформаційної безпеки

До таких заходів можна віднести:

— підготовку пакета організаційно-розпорядчих документів щодо захисту інформації;
— встановлення форми реєстрації осіб, які офіційно отримували доступ до даних (хто, коли, з якою метою і на яких підставах);
— встановлення форм обліку зібраної або переглянутої інформації із зазначенням цілей і підстав таких дій;
— визначення основних напрямів і методів здійснення контролю за роботою персоналу, який працює з даними;
— складання переліку посадових осіб, на яких доцільно покласти відповідальність за захист персональних даних, у тому числі законність їх передачі та використання третіми особами;
— ознайомлення персоналу з вимогами інформаційної безпеки при обробці даних, а також надання зобов'язання про нерозголошення відомостей, які стали відомі в результаті здійснення своїх функцій;
— проведення навчання працівників з питань інформаційної безпеки та подальше тестування персоналу з метою оцінювання рівня знань;
— встановлення обмеженого режиму доступу до приміщень з технічним обладнанням.

Варто звернути увагу, що це не повний перелік необхідних заходів. Кожна установа визначає його самостійно.

2. Які існують заходи фізичної безпеки щодо доступу до даних?

До заходів фізичної безпеки належать:

1. ***Режим доступу до приміщень.*** Вхід до кімнат, де обробляються дані, дозволений лише особам, які мають відповідний рівень доступу.
2. ***Контроль за відвідувачами.*** Усі відвідувачі повинні реєструватися у відповідних журналах чи електронному реєстрі і вказувати мету відвідування.

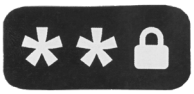
3. ***Захист обладнання та документів.*** Обладнання має бути захищене так, щоб мінімізувати ризики неконтрольованого доступу до нього. Необхідно унеможливити фотографування або перегляд зображення на моніторах сторонніми особами, а також використання ними флешнакопичувачів (з метою уникнення несанкціонованого копіювання інформації з комп'ютера або його ураження «вірусом» чи іншою шкідливою програмою). Відвідувачам має бути взагалі заборонено вносити, а персоналу — виносити електронні носії інформації. Кожна така спроба повинна фіксуватися та стати підставою для службового розслідування. Подібні заходи безпеки стосуються й паперових документів.

3. Для чого потрібна ідентифікація та автентифікація під час обробки даних?

Цифрова трансформація передбачає, що процес обробки персональних даних швидко й невпинно переходить у цифровий формат, що цілком обґрунтовано, адже набагато зручніше й простіше корегувати, зберігати, систематизувати, передавати дані в електронному форматі.

Водночас обробка даних за допомогою сучасних технологій і їх зберігання в інформаційних системах призвела до нових викликів у сфері їх охорони. Викрасти, знищити чи спотворити інформацію стало можливо шляхом віддаленого натискання кількох кнопок на клавіатурі, а звичайна флешка дозволяє зловмиснику винести в кишені інформацію обсягом з невелику бібліотеку.

Як уже було зазначено вище, працювати з базами персональних даних повинне чітко визначене коло осіб, які здобули належну кваліфікацію й офіційно несуть відповідальність за безпеку довіреної їм інформації, у тому числі й тієї, що зберігається в електронному вигляді. Це означає, що доступ до інформаційних систем з персональними даними повинен бути врегульований і контрольований. Тобто користувач повинен підтвердити своє право користуватися системами — пройти *процедури ідентифікації та автентифікації*.



Ідентифікація — це пред'явлення користувачем системі своїх індивідуальних й унікальних ідентифікаторів, як правило, логіну (реєстраційне ім'я) і паролю входу.

Автентифікація — це процедура впізнання системою наданих ідентифікаторів. Простіше кажучи, користувач через

комп'ютер вводить у систему свій логін і пароль, отримавши їх, система проводить автентифікацію, порівнюючи їх з логіном і паролем, наявним у базі даних, щоб переконатися в тому, що користувач саме той, за кого себе видає.

Правила безпечного використання пароля передбачають:

— збереження його конфіденційності;
— відсутність відображення пароля на екрані під час його введення;
— заборону використання одного пароля кількома користувачами;
— зміну пароля у випадку наявності ознак можливої компрометації системи або пароля;
— блокування доступу після кількох спроб введення неправильного пароля;
— зберігання історії попередніх призначених для користувача паролів у формі hash (за попередній рік) і запобігання їх повторному використанню.

Увівши логін і пароль входу в систему, користувач створює власний *обліковий запис*. За допомогою такого запису відстежуються всі його дії в системі: час входу та виходу з неї, адреса використаного для цього комп'ютера, частота перебування в системі та проведені в ній операції.

Так, *реєстрація спроб входу / виходу* користувачів із системи повинна фіксувати:

1. дату і час спроби входу / виходу;
2. ідентифікатор користувача;
3. результат спроби: успішна чи невдала.

Реєстрацію виконаних операцій необхідно здійснювати за такими параметрами:

1. дата і час виконання операції (найменування операції);
2. ідентифікатор користувача;
3. зміст операції (перегляд, корегування, запис, видалення та ін.);
4. результат спроби виконати операцію: успішна чи невдала.

Реєстрація зміни права доступу користувача має відобразити:

1. дату і час зміни повноважень;
2. ідентифікатор адміністратора, що здійснив зміни, його нові повноваження (рівень доступу) і статус.

Використання індивідуальних паролів має гарантувати, що доступ до персональних даних отримають лише ті люди, які мають на це право. А отже, їх розголошення в будь-який спосіб не припустиме, хоча подібні

випадки ще трапляються. Так, в одному з підрозділів ОМС пароль входу у систему був написаний на стікері, який наклеїли на монітор комп'ютера.

В іншому ОМС працівник по роботі з персоналом повідомив свій логін і пароль входу до інформаційної бази студентам-практикантам, потім пояснивши свій вчинок тим, що *«вони краще розуміються на комп'ютерах і швидше проведуть систематизацію файлів».*

4. Як фіксувати випадки несанкціонованого витоку даних?

До інцидентів безпеки можна віднести будь-які випадки, що загрожують процесам обробки та безпеки персональних даних — від ненавмисного залишення користувачем комп'ютера з інформацією увімкнутим до хакерської атаки для знищення файлів.

Серед найбільш поширених видів інцидентів безпеки можна виділити такі:

— неавторизований або несанкціонований доступ третіх осіб до інформаційної системи;
— відмова обладнання через причини технічного характеру;
— порушення роботи програмного забезпечення;
— недотримання персоналом правил обробки, зберігання, передачі інформації;
— виявлення фактів зовнішнього моніторингу або встановлення контролю над роботою системи чи окремих її елементів;
— ураження вірусами або іншими шкідливими програмами;
— будь-яка компрометація системи, наприклад «зламування» та оприлюднення пароля облікового запису.

Частина інцидентів може бути малопомітною, проте вони не повинні залишатися поза увагою, адже їх частота появи й загальна кількість — один з показників ефективності захисту персональних даних. З урахуванням цього всі зафіксовані інциденти безпеки мають бути класифіковані за ступенем загрози, описані, піддані всебічному аналізу для розроблення заходів з усунення причин їх виникнення надалі.

Адміністрування інцидентів інформаційної безпеки базується на таких діях:

1. ***Встановлення*** — з урахуванням викладених у регламенті критеріїв визначається, чи є певна подія (дія) інцидентом безпеки.

2. ***Реагування*** — в особливих випадках інциденти безпеки вимагають невідкладного реагування, наприклад відключення обладнання,

блокування доступу до бази даних тощо. Причини для такого реагування та механізм здійснення повинні бути заздалегідь визначені в регламенті.

3. ***Оповіщення*** — якщо подія (дія) ідентифікована як інцидент, персонал інформує про нього за встановленою регламентом формою відповідну посадову особу (керівника органу, начальника служби безпеки тощо).

4. ***Реєстрація*** — факт встановлення інциденту безпеки фіксується офіційно в реєстрі, журналі або в інший спосіб, передбачений регламентом.

5. ***Усунення причин і наслідків*** — вжиття невідкладних заходів з припинення впливу інциденту безпеки на обробку персональних даних і відновлення їх належного захисту. При цьому слід враховувати те, що такі заходи не повинні знищувати докази наявності інциденту, які будуть необхідні для проведення розслідування причин виникнення інциденту.

6. ***Розслідування*** — вивчення умов та обставин, що зумовили або сприяли виникненню інциденту безпеки.

Під час розслідування потрібно:

— встановити причини виникнення інциденту й недоліки в організаційно-розпорядчих документах, які уможливили його;

— зібрати й оформити докази та інші фактичні дані, які підтверджують факт інциденту;

— встановити мотиви скоєння інциденту та винуватих осіб, чиї умисні дії або недбалість призвели до інциденту;

— виявити замовника інциденту та можливу причетність до нього сторонніх осіб;

— встановити наслідки інциденту та завдану ним шкоду.

У межах службового розслідування перевіряються всі носії інформації (реєстри, журнали обліку тощо) та аналізуються дії користувачів, які мали доступ до систем у період виникнення інциденту безпеки. За результатами розслідування готується протокол або акт комісії, а у випадку, коли в інциденті встановлені ознаки скоєння правопорушення, про нього повідомляються органи правопорядку, куди передаються всі отримані матеріали.

7. ***Превенція*** — реалізація заходів, які мінімізують ризики повторного виникнення подібної ситуації.

8. ***Аналітика*** — ґрунтовний аналіз інциденту, на підставі якого здійснюється загальне вдосконалення захисту персональних даних.

Превентивні заходи для протидії витоку персональних даних мають особливе значення у воєнний час і при загрозі окупації. Масштаби та хід бойових дій важко спрогнозувати, а тому в будь-якому випадку потрібний чіткий план дій відповідального працівника в разі настання подібних обставин.

5. Які існують заходи для здійснення внутрішнього контролю?

До заходів внутрішнього контролю можна віднести такі:

— опитування та співбесіди з персоналом ОМС з метою з'ясування їхньої думки про наявний рівень захисту персональних даних;

— огляд робочих місць працівників, використовуваного ними обладнання та програмного забезпечення;

— перевірка відповідних реєстрів і службової документації;

— тестування технічних засобів обробки та захисту персональних даних;

— штучне моделювання інцидентів інформаційної безпеки та виникнення виняткових ситуацій з метою напрацювання алгоритму дій персоналу в таких обставинах;

— проведення навчальних і просвітницьких заходів у цій сфері з обговоренням ключових проблем, які виникають під час обробки даних, і можливих шляхів їх розв'язання.

Ефективним засобом контролю за дотриманням норм законодавства при обробці персональних даних є *зовнішній аудит інформаційної безпеки*, який дає можливість більш об'єктивно оцінити рівень захисту даних і визначити потенційні загрози для них. Аудит полягає в ґрунтовному вивченні стану безпеки інформації в системі за допомогою залучення фахівців, які надають відповідні консалтингові послуги.

ВИСНОВОК

Забезпечення права людини на приватне життя — це набагато більше, ніж вивішена в холі ОМС табличка «Ведеться відеоспостереження» та папірець на інформаційному стенді з повідомленням про обробку даних. Передусім це становлення нової культури взаємовигідних відносин між ОМС і мешканцем громади. Культури, яка передбачає взаємну довіру, розуміння посадовцями всього спектру вразливості людини в інформаційному середовищі та усвідомлення своєї відповідальності за її належний захист.

ДЖЕРЕЛА ПРАВОВОГО РЕГУЛЮВАННЯ

1. Стаття 32 Конституції України
2. Стаття 12 Загальної декларації прав людини
3. Стаття 17 Міжнародного пакту про громадянські і політичні права, ратифікованого указом Президії Верховної Ради УРСР від 18 вересня 1973 року № 2148-VIII (2148-08)
4. Стаття 8 Конвенції про захист прав людини і основоположних свобод
5. Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних і Додатковий протокол до неї, ратифіковані Законом України від 6 липня 2010 року № 2438-VI
6. Директива № 2002/58/ЄС Європейського Парламенту і Ради ЄС «Про обробку персональних даних та захист таємниці сектора електронних комунікацій» від 12 липня 2002 року
7. Директива № 95/46/ЄС Європейського Парламенту і Ради ЄС «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 року
8. Закон України «Про захист персональних даних»
9. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»
10. Закон України «Про доступ до публічної інформації»
11. Стаття 188-39 «Порушення законодавства у сфері захисту персональних даних» і стаття 188-40 «Невиконання законних вимог Уповноваженого Верховної Ради України з прав людини» Кодексу України про адміністративні правопорушення
12. Стаття 182 «Порушення недоторканності приватного життя» Кримінального кодексу України
13. Рішення Конституційного Суду України від 20 січня 2012 року № 2-рп/2012
14. Постанова Пленуму Вищого адміністративного суду України від 29 вересня 2016 року № 10 «Про практику застосування адміністративними судами законодавства про доступ до публічної інформації»

15. Типовий порядок обробки персональних даних, затверджений наказом Уповноваженого Верховної Ради України з прав людини «Про затвердження документів у сфері захисту персональних даних» від 8 січня 2014 року № 1/02-14

16. Порядок здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних

17. Порядок повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних при їх обробці, а також оприлюднення вказаної інформації

18. Роз'яснення Уповноваженого Верховної Ради України з прав людини щодо особливостей реалізації права на доступ до публічної інформації в умовах воєнного стану

19. Guidelines on Data Protection Impact Assessment (DPIA)

20. Офіційний переклад Регламенту Європейського Парламенту і Ради (ЄС) 2016/679 про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних та про скасування Директиви 95/46/ЄС

21. AEPD, The Practical Guide for Data Protection Impact Assessments Subject to the GDPR

22. Standards ISO-29134 «Guidelines for privacy impact assessment», ISO-31000 «Risk management. Principles and guidelines», ISO-31010 «Risk management. Risk assessment techniques»

23. ICO, Data Protection Impact Assessments

24. EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (Version 2.0, Oct 2020)

25. Center for Information Policy Leadership (CIPL), Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR (Dec 2016)

КОРИСНІ ПОСИЛАННЯ

— **Методичний посібник «Аналіз ризиків під час обробки персональних даних: що важливо знати?»** (про етичні принципи та підходи до створення системи захисту даних). Режим доступу до ресурсу: https://umdpl.info/wp-content/uploads/2021/09/Posibnyk_otsinka-ryzykiv-ZPD_na-sajt.pdf

— **Правовий аналіз права людини на своє зображення** (аналітика про регулювання публікацій фото в мережі). Режим доступу до ресурсу: https://helsinki.org.ua/wp-content/uploads/2022/01/Personal_Photo_A5.pdf

— **Історична хронологія, коли люди почали боротися за свою приватність.** Режим доступу до ресурсу: https://zmina.info/columns/pravo-na-pryvatne-zhyttya-istoriya-rozvytok-ukrayinski-realiyi/?fbcl

— **Роз'яснення, що треба знати про право на приватність під час відеонагляду в магазині, супермаркеті, на робочому місці тощо.** Режим доступу до ресурсу: https://ombudsman.gov.ua/storage/app/media/ЗПД/rozyasnennya.pdf

— **Методичний посібник «Відеоспостереження у публічних місцях».** Режим доступу до ресурсу: https://umdpl.info/wp-content/uploads/2021/09/POSIBNYK_videosposterezhennya_u_publichnyx_miscyax.pdf

— **Рекомендації Уповноваженого Верховної Ради України з питань додержання конституційного права людини і громадянина на доступ до інформації.** Режим доступу до ресурсу: https://rm.coe.int/recomendations-final-10-02-21/1680a165f7

— **Рекомендації Уповноваженого Верховної ради України з прав людини з питань додержання права на доступ до інформації** (порадник для територіальних громад). Режим доступу до ресурсу: https://www.undp.org/uk/ukraine/publications/rekomendatsiyi-upovnovazhenoho-verkhovnoyi-rady-ukrayiny-z-prav-lyudyny-z-pytan-doderzhannya-prava-na-dostup-do-informatsiyi?fbclid=IwAR0lfyFNpJ1-xSFZkTmMKMQgQR3GDIn86xiW1mvRd-Mr_XfhsZOcsqgQK3Es