АНАЛІЗ РИЗИКІВ ПІД ЧАС ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ:

ЩО ВАЖЛИВО ЗНАТИ?

Асоціація УМДПЛ UMDPL Association

Аналіз ризиків під час обробки персональних даних: що важливо знати?/ У.С. Шадська. — К.. Компринт, 2021. — 68 с.

Авторка: **Уляна Шадська**

Літературна редакторка: **Мар'яна Добоні**

Дизайн та верстка: **Іван Юрчик**

У цьому посібнику посадові особи органів місцевого самоврядування та підпорядкованих їм установ можуть ознайомитися з положеннями законодавства про захист персональних даних і процедурами оцінювання ризиків під час їх обробки.

Викладені рекомендації базуються на положеннях національного та міжнародного законодавства, що робить цей методичний матеріал актуальним для інших суб'єктів, які обробляють персональні дані.

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

© Асоціація УМДПЛ, 2021

ЗМІСТ

ВСТУП 4

РОЗДІЛ 1 12

1.1. Основні поняття 13

1.2. Принципи обробки персональних даних 14

1.3. Підстави для обробки персональних даних 17

1.4. Проєктування дизайну приватності 19

РОЗДІЛ 2 22

2.1. Поняття «аналіз ризиків» 24

2.2. Ризики, які необхідно оцінювати 27

2.3. Індикатори, які визначають ступінь ризику 29

2.4. Етичні принципи під час застосування цифрових технологій 36

РОЗДІЛ 3 42

3.1. Ключові кроки процесу аналізу ризиків 43

3.2. Учасники процесу аналізу ризиків 52

3.3. Публікація результатів оцінювання впливу на захист даних 52

ВИСНОВКИ 54

ДЖЕРЕЛА 57

ДОДАТОК 1 58

ДОДАТОК 2 60

ДОДАТОК 3 64

ВСТУП

Сучасна тенденція діджиталізації державних послуг торкнулася не тільки центральних органів виконавчої влади, а й місцевого самоврядування, які здійснюють управління суттєвою часткою суспільних справ в інтересах 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 та ін. Це означає, що для виконання своїх функцій органи місцевого самоврядування (далі — ОМС) збирають й обробляють великі обсяги персональних даних населення.

З кожним роком ОМС ухвалюють нові технологічні й організаційні рішення для вдосконалення для своєї діяльності. Зокрема, поступово впроваджують елементи технологічної інфраструктури: послуги, які надаються в мережі; системи електронного документообігу; офіційні вебсайти; апаратні комплекси систем відеоспостереження для підтримки публічної безпеки на місцях та ін. Але розвиток технологій, окрім переваг, має великий спектр ризиків для недоторканності приватного життя людини.

У зв'язку з цим усе гостріше постає питання про необхідність встановлення чітких правил роботи з персональними даними та запровадження ефективних процедур оцінювання всіх можливих ризиків для прав і свобод людини під час їх обробки.

Потрібно зауважити, що згідно з міжнародними стандартами[1] процес обробки та захисту персональних даних має ґрунтуватися на підході, де всі суб'єкти, які збирають конфіденційну інформацію, повинні здійснювати систематичні заходи з оцінювання ризиків. Такі вимоги зазначені і в європейському законодавстві[2] та законодавстві інших країн світу.

Мова йде про запровадження в практичну діяльність інструмента для виявлення та реагування на загрози для людини під час

---

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

2 Необхідність проведення оцінювання впливу на захист даних, або Data Protection Impact Assessment (DPIA), передбачена статтею 35 Загального регламенту захисту даних та іншими документами.

роботи з її даними. Глибокий аудит дозволяє зрозуміти, як функціонує інформація в установі та що треба зробити, щоб покращити цей процес для дотримання цифрового законодавства.

Масштаби й діапазон роботи з інформацією в кожному ОМС різняться. Водночас принципи та алгоритми захисту інформації залишаються єдиними, оскільки типові ризики її втрати, знищення чи неконтрольованого витоку достатньо давно відомі та описані. Поняття «ризик» не слід пов'язувати лише з «людським фактором», адже до виникнення інцидентів інформаційної безпеки можуть призвести й інші чинники.

Повністю уникнути ризиків й убезпечити зібрану інформацію в умовах сучасного цифрового світу складно. Водночас передбачити потенційні загрози, своєчасно виявляти, мінімізувати та певною мірою навіть управляти ними — цілком можливо.

Саме з такою метою й підготовлено цей посібник. За його допомогою посадові особи ОМС зможуть отримати базові знання про порядок, цілі та принципи оцінювання ризиків під час обробки персональних даних.

Немає єдиного шаблона, за яким це найкраще здійснювати. Як правило, кожна установа або її структурний підрозділ розробляє індивідуальну методологію, яка враховує специфіку її діяльності та потреби. У цьому виданні розглянуто загальні підходи, які допоможуть сформувати власний сценарій аналізу ризиків, щоб надалі розвивати таку практику.

Зазначимо, що в цьому методичному матеріалі інформаційна безпека розглядається крізь призму міжнародних стандартів і сучасних європейських правил, встановлених Загальним регламентом про захист даних, який набрав чинності в країнах Європейського Союзу (далі — ЄС) з 25 травня 2018 року. Особливістю Регламенту є те, що його дія поширюється не тільки на територію ЄС, а й організації, які базуються за його межами. Таким чином, навіть несвідоме ігнорування його вимог в Україні може поставити під загрозу налагодження зв'язків і співпрацю з європейськими партнерами, оскільки така взаємодія передбачає обмін інформацією між сторонами.

Метою обробки персональних даних є служба людству — *наголошується у Регламенті. Рано чи пізно, але діяльність*

усіх органів влади й місцевого самоврядування буде відповідати цій простій тезі. І починати готуватися до таких змін треба вже зараз[3].

Окремі факти з історії

Цікаво, що саме з розуміння ризиків для людини й почалася історія розвитку права на недоторканність приватного та сімейного життя. Суворий європейський підхід до приватності людини, який ми бачимо сьогодні, перегукується з трагічними подіями Другої світової війни, коли нацисти збирали особисті дані для ідентифікації євреїв та представників інших меншин[4]. У 1930-х роках у Німеччині провели перепис населення, вказуючи в картках національність, рідну мову, релігію та професію жителів. Уся ця інформація систематизувалася за допомогою перших процесорів, відомих як Hollerith, що встановлювалися німецькою філією компанії International Business Machines (далі — IBM).

Цей історичний факт став відомим після публікації у 2001 році документальної книги журналіста Едвіна Блека «IBM і Голокост», у якій детально описані відносини компанії IBM з урядом Адольфа Гітлера в період Другої світової війни. У книзі розповідається, як за допомогою технологій здійснювався геноцид єврейського народу. Вони не тільки ідентифікували та затримували людей, а й управляли поїздами, щоб доставляти їх у концентраційні табори. Тоді людству стало зрозуміло, що технології, особливо ті, які використовує держава, можуть бути як корисними, так і завдавати шкоди людям, усе залежить від мети їх застосування.

У 1948 році право на приватне та сімейне життя зафіксовано в статті 12 Загальної декларації прав людини, а в 1950 році — у статті 8 Європейської конвенції з прав людини і основоположних свобод. З огляду на сумні історичні приклади в Раді Європи дійшли висновку, що потрібно максимально регламентувати технологічну діяльність. У 1968 році Парламентська Асамблея опублікувала

3 Володимир Батчаєв, Асоціація УМДПЛ.

4 The GDPR Is Just the Latest Example of Europe's Caution on Privacy Rights. That Outlook Has a Disturbing History: *https://time.com/5290043/nazi-history-eu-data-privacy-gdpr/*

рекомендації щодо усунення загроз правам людини в результаті використання автоматизованої обробки персональних даних. Це спонукало до того, що у 1970 році на західнонімецькій землі Гессен ухвалили закон про конфіденційність даних у державному секторі. Це був локальний акт, який застосовувався лише на території цієї землі. Трьома роками пізніше подібний закон ухвалено у Швеції — Datalgen (букв. Data Act). На відміну від німецького цей акт регулював тільки приватний сектор, тому навряд чи можна сказати, що він захищав права людей, радше навпаки — його функція полягала в тому, щоб контролювати їх.

У 1977 році Німеччина все ж таки стала першою країною, яка ухвалила на федеральному рівні повноцінний закон про захист персональних даних, який був покликаний захищати приватність людини[5]. До сьогодні Німеччина вважається одним зі світових лідерів у сфері захисту приватного життя. Наступною була Франція, яка ухвалила в 1978 році закон про інформатику та громадянські свободи. Німецький і французький акти дали значний імпульс для розвитку сфери захисту персональних даних у Європі. На цю проблему почали звертати увагу більше країн і міжнародних організацій.

У 1995 році ЄС ухвалив Директиву 95/46/ЄС «Про захист фізичних осіб під час оброблення персональних даних і про вільне переміщення таких даних», яка стала основою законодавства країн ЄС. Цей документ визначив загальні принципи захисту даних, а також наділив людей правом знати, яка інформація про них збирається, де зберігається і з якою метою. На основі цієї директиви були ухвалені локальні акти майже в усіх країнах ЄС, а згодом, у 2010 році, і в Україні.

Таким чином, понад століття тому суспільство заговорило про захист даних у зв'язку з тим, що робить цю тему популярною й зараз, — розвитком технологій, які становлять ризики для прав і свобод людини. Усе більше особистої інформації підпадає під автоматичну обробку, зокрема з використанням штучного інтелекту. У 1990-х роках сформувалися основні корпорації-гіганти, відомі також як «велика п'ятірка», або GAFAM (Google, Amazon, Facebook, Apple, Microsoft), які почали продавати рекламу, ґрунтуючись на

5 Bundesdatenschutzgesetz (1977).

аналізі поведінки своїх користувачів[6]. Такий спосіб прямої капіталізації швидко став популярним, бо компанії зрозуміли цінність персональних даних і скільки на них можна заробляти. Щороку покращується система аналізу та збираються дедалі більші обсяги інформації про людей з усього світу. Понад те, такі технології почали широко використовувати не тільки бізнес-структури, а й державні та місцеві органи влади.

Уряди різних країн оцінили ризики від такої діяльності для прав людини, і у 2002 році ЄС ухвалив Директиву ePrivacy, яка регламентує використання всіх програм, зокрема відомих нам cookies, які збирають дані для реклами або іншої маркетингової діяльності в мережі. Часто помилково вважають, якщо держаний або інший орган влади нічого не продає на своїх вебресурсах, значить не здійснює електронну рекламу. Проте, згідно з висновками міжнародних урядових і неурядових організацій, будь-яка дія або повідомлення, які мають на мені вплинути на поведінку людини (щось купити, підтримати, зробити тощо), підпадає під це поняття.

Тому у 2014 році Європейський Суд підтвердив право людини вимагати видалення своїх особистих даних з пошукових систем, які видаються неадекватними або більше неактуальними[7].

На початку 2000-х років у світі почали широко обговорювати загрози витоків даних, масового стеження та кіберзагрози. Серед знакових прикладів — сенсаційна заява колишнього співробітника АНБ[8] Едварда Сноудена про те, як розвідка США стежить за людьми всередині країни та за її межами; історія консалтингової компанії Cambridge Analytica, яка зламала дані понад 50 млн облікових записів Facebook, щоб вплинути на результат президентських виборів у США у 2016 році та кампанію виходу Великої Британії з ЄС. Усі ці та інші події стали поштовхом для розробки та ухвалення нового законодавства, яке змусить державні органи чи приватні компанії належно захищати персональні дані, які вони збирають.

---

6 Так званий таргетинг.

7 *https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf*

8 Агентство національної безпеки — агентство криптологічної розвідки США, яке є частиною Міністерства оборони США і відповідає за збір та аналіз іноземної розвідувальної інформації.

25 травня 2018 року набув чинності Загальний регламент захисту даних (далі — GDPR, Регламент)[9]. Цей закон став одним з найжорсткіших у сфері захисту приватності людини за останні 20 років. GDPR визначив нові європейські стандарти з питань захисту персональних даних, замінивши ухвалену раніше рамкову Директиву 95/46/ЄС. Він спрямований на те, щоб у людини було більше законодавчих інструментів здійснювати контроль над власними даними. Норми GDPR можуть бути застосовані не тільки до суб'єктів, що перебувають на території ЄС[10].

Глобальний вплив GDPR неможливо переоцінити. Більшість з понад шістдесяти країн, які в останнє десятиліття ухвалили нові закони про конфіденційність даних, розташовані в Африці, Азії та Америці, майже всі вони змоделювали свій підхід на основі європейського Регламенту та його попередниці — Директиви 95/46/ЄС. Усе більше країн світу ухвалюють за основу національного законодавства модель GDPR, що демонструє усвідомлення ризиків неправомірного використання персональних даних. Більшість країн світу прагнуть встановити єдині правила роботи з інформацією та усунення можливих загроз для людини та держави загалом[11]. Наприклад, у червні 2021 року президент США Джозеф Робінетт Байден-молодший підписав розпорядження про захист чутливих даних американців від іноземних супротивників, у якому зазначено необхідність розробки заходів з «ліквідації надзвичайних ситуацій на національному рівні в контексті використання інформаційних технологій». Зокрема, ідеться про постійне оцінювання на різних рівнях державного управління у сфері захисту від ризиків при доступі до даних і формуванні процедур постачання, транзакцій і розробки програмних додатків[12].

---

9 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: *https://www.kmu.gov.ua/storage/app/media/uploaded-files/es-2016679.pdf*

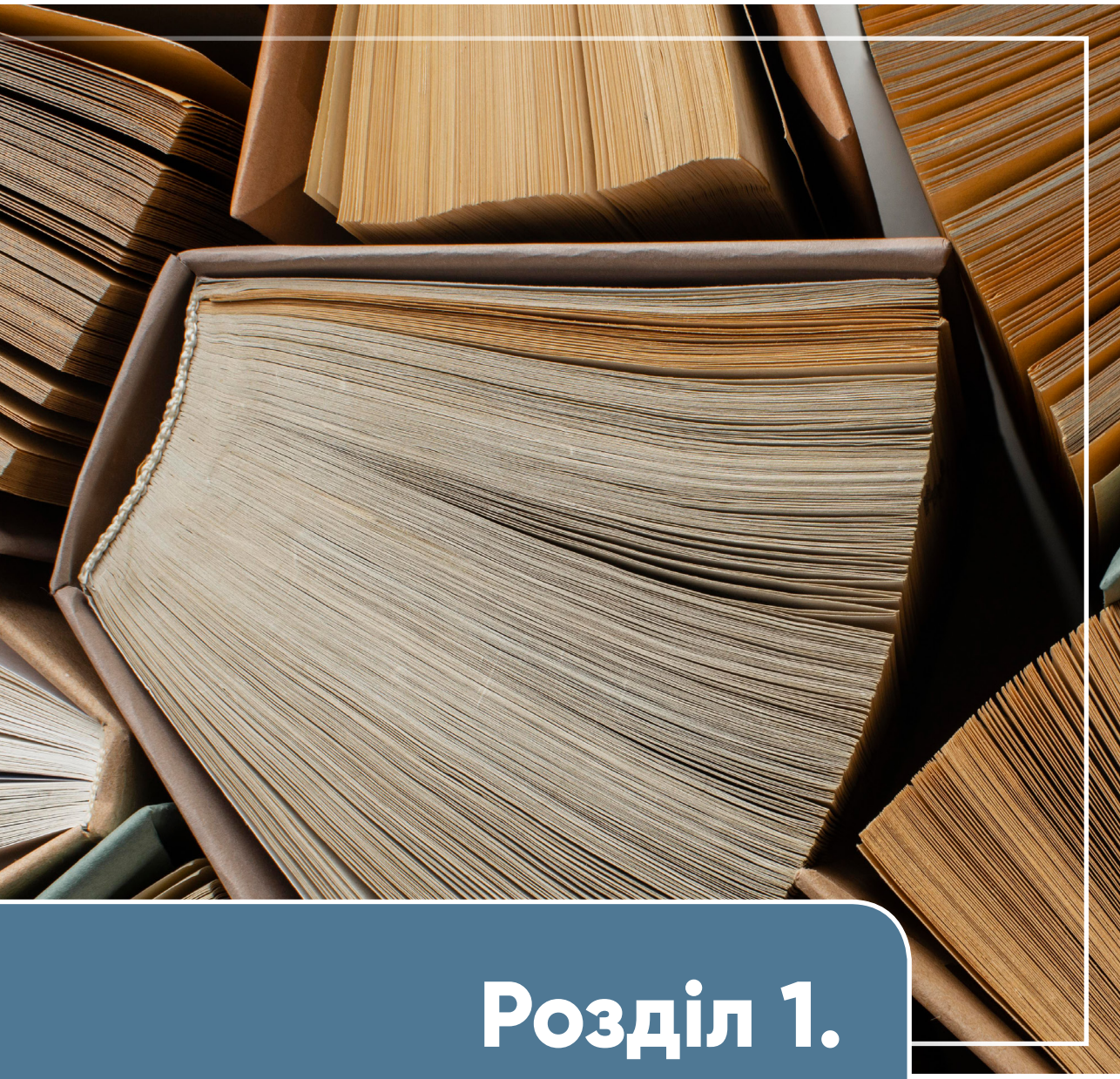
10 Стаття 3 Регламенту.

11 Уляна Шадська. Право на приватне життя: історія, розвиток, українські реалії, ZMINA, 2021.

12 Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries: *https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/09/executive-order-on-protecting-americans-sensitive-data-from-foreign-adversaries/?fbclid=IwAR21NGlq5rCk69-8pgxsIFBlfpfebKm3bMZ0s2alrShLkqcEYOaSSK6zlkg*

Останніми роками в Україні також активно обговорюють необхідність реформ у сфері захисту персональних даних. Право на повагу до приватного життя закріплено в статті 32 Конституції України. У 2011 році набрав чинності Закон України «Про захист персональних даних», написаний за зразком Директиви 95/46/ЄС, тому за своїм змістом він схожий з європейським. Проте на момент його ухвалення користування інтернетом і технологіями ще не було настільки поширено, як зараз. Цифрова трансформація різних сфер посилила необхідність модернізації законодавства. Понад те, у 2014 році Україна взяла на себе зобов'язання в межах Угоди про асоціацію з ЄС забезпечити належний рівень захисту даних відповідно до міжнародних стандартів, документів Ради Європи[13]. Це ще одна обґрунтована підстава для того, що не варто чекати тотальної уніфікації, а вже сьогодні діяти за єдиним міжнародним протоколом.

13 Стаття 15 Угоди.



Розділ 1.

Загальні положення та термінологія в законодавстві

Робота ОМС завжди пов'язана з обробкою певного виду інформації[14], значна частина якої містять персональні дані. Щоб зрозуміти, чи належно здійснюється обробка конфіденційної інформації (будь-якої іншої), потрібно розібратися зі змістом термінів і правил у законодавстві, а також з напрямками діяльності, які можуть становити ризик для прав і свобод людини.

1.1. Основні поняття

Що таке «персональні дані»?

Персональні дані[15] — це відомості чи сукупність відомостей про фізичну особу, які дають можливість прямо або опосередковано її ідентифікувати. Тобто йдеться про будь-яку інформацію про людину. Вона може бути у формі цифр; фото (зображення людини); відео; звуку (голос); IP-адреси, кодів тощо.

Персональні дані поділяють на дві категорії — загальну й особливу.

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

Особлива категорія розкриває інформацію про расове або етнічне походження, політичні та релігійні переконання, приналежність до політичних партій, наявність судимості за вчинення правопорушення, а також дані, що стосуються здоров'я, статевого життя, біометричних особливостей[16].

У законодавстві різних країн світу загальний масив інформації неспроста розділили на дві категорії. З огляду на зміст особливої категорії така інформація може становити більший ризик для людини, тому встановлені окремі правила роботи з нею. Серед основних критеріїв необхідності здійснення процедури оцінювання ризиків в організації — обробка особливої (або ще спеціальної,

---

14 Службової, конфіденційної чи, можливо, таємної.

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

16 У статті 7 Закону України «Про захист персональних даних» вказано вичерпний перелік особливої категорії даних.

чутливої) категорії даних. Отже, під час обробки даних необхідно враховувати їх категорію та застосовувати відповідні рівні безпеки.

Що таке обробка персональних даних?[17]

Обробка персональних даних — це будь-яка дія з ними: збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання, поширення, реалізація, передача, знеособлення та знищення.

Часом можна натрапити на вислів «життєвий цикл даних», тобто те, як функціонує інформація в організації (або окремий її вид). Залежно від форми та способу обробки оцінюватиметься потенційний ризик. Наприклад, одні дані організації необхідні лише для збереження, тоді як інші для передачі та розповсюдження.

1.2. Принципи обробки персональних даних

Міжнародними стандартами визначено основні принципи обробки персональних даних, які є фундаментом для врегулювання цієї сфери. Будь-яка методологія оцінювання ризиків буде передусім ґрунтуватися на питаннях, чи дотримано загальноприйнятих принципів роботи з інформацією.

Що це за принципи?

1. Законність, справедливість і прозорість

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

Справедливість полягає в тому, що при обробці даних потрібно враховувати права людини, не завдавати шкоди її законним інтересам, а також запобігати будь-яким зловживанням з боку володільця чи розпорядника персональних даних.

Прозорість гарантує право людини на отримання інформації про обробку її персональних даних. Тому необхідно пояснювати в доступній формі широкому загалу для чого, яким чином ці дані

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

збираються, як вони будуть використовуватися та кому вони можуть бути передані.

З'ясувати, чи дотримано ці принципи, можна за допомогою питань (у контексті процесу оцінювання ризиків):

- Чи є законна підстава для збору та подальшої обробки персональних даних?[18]
- Чи визначені окремі умови обробки та безпеки для особливої категорії даних?
- Чи розглянуті перед початком роботи сценарії, як може вплинути обробка на суб'єктів, чиї дані збираються?
- Обробка інформації здійснюється тільки в межах визначених цілей?
- Чи було поінформовано про це осіб, чиї дані збираються?

2. Обмеження мети

Персональні дані можуть збиратися лише з конкретною та законною метою і лише тоді, коли без такої інформації досягнення мети неможливе. Саме від цілей збору даних залежить обсяг і спосіб їх обробки, а не навпаки. Принцип обмеження мети вимагає заздалегідь визначити та обґрунтувати підстави й мету збору даних, адже надалі це стане запобіжником від їх використання з незаконною метою.

З'ясувати, чи дотримано цей принцип, можна за допомогою таких питань:

- Чи визначено мету та завдання обробки даних?
- Чи задокументовано ці цілі?
- Чи збір інформації здійснюються лише в межах визначеної мети?

3. Мінімізація даних

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

---

18 Підстави для обробки персональних даних визначені у статті 11 Закону України «Про захист персональних даних».

З'ясувати, чи дотримано цей принцип, можна за допомогою таких питань:

- Чи дані збираються тільки для досягнення конкретних цілей (немає надлишкових даних)?
- Чи здійснюється аналіз обсягу даних?
- Чи існує процедура видалення надлишкових даних?

Тобто, наприклад, якщо формується база персональних даних (наприклад, номерів телефонів, електронних адрес тощо) для організації навчального семінару, то не потрібно додатково збирати адреси місця реєстрації проживання людей. У разі, якщо така інформація збирається, це потрібно обґрунтувати. Іншими словами, принцип полягає в тому, що не варто збирати дані лише на випадок, що вони можуть стати в пригоді в майбутньому.

4. Точність

Цей принцип вимагає контролювати правильність й актуальність отриманих персональних даних. Застарілі або неточні дані підлягають виправленню або знищенню у спосіб, що виключає можливість їх поновлення.

Перевірити, чи дотримано цей принцип, можна за допомогою таких питань:

- Чи гарантована точність будь-яких персональних даних, які збираються?
- Чи впроваджені відповідні процеси для перевірки точності зібраних даних?
- Чи існує процес, що дозволяє визначити, коли потрібно оновлювати дані для належного виконання визначеної мети?
- Чи забезпечено процедури реалізації права людини на виправлення даних у разі їх неточності чи неактуальності?

5. Обмеження строку зберігання

Персональні дані мають зберігатися не довше, ніж це необхідно для досягнення мети їх обробки. Коли таку мету досягнуто, дані повинні бути видалені чи знищені. Зберігання даних протягом більш тривалого часу допускається, якщо це необхідно для громадських інтересів, з науковою метою, задля історичних досліджень або формування статистики. Також у разі необхідності тривале

зберігання даних можна здійснювати після їх знеособлення, тобто переведення у вигляд, який не дає можливості ідентифікувати особу.

6. Цілісність і конфіденційність (безпека)

Обробка персональних даних повинна здійснюватися в спосіб, який гарантує їх належну безпеку, зокрема від несанкціонованих / незаконних дій з ними або випадкової втрати. Суб'єкти, що збирають або обробляють дані, несуть повну відповідальність за реалізацію заходів з їх захисту.

7. Підзвітність (або принцип відповідальності)

ОМС і підпорядковані їм установи повинні документувати свою діяльність і бути готовими продемонструвати правомірність своїх дій у сфері захисту персональних даних. Зрозуміло, що компетентні органи відповідно до своїх повноважень можуть здійснювати перевірку стану дотримання закону в цій сфері, але підзвітність у широкому розумінні — це засіб демонстрації суспільству, яким чином забезпечується захист інформації.

Дотримання принципу підзвітності допомагає здобути довіру людей, оскільки його суть — максимально показати, як забезпечується повага до приватного життя людини та які здійснюються заходи зі зниження можливих ризиків його порушення.

Підсумовуючи, зауважимо, що всі сім принципів тісно пов'язані й доповнюють один одного, утворюючи єдину концепцію дотримання прав людини під час обробки персональних даних[19]. Якщо хоч один з цих принципів не буде враховано в діяльності організації, тоді це можна вважати сигналом про можливі порушення інформаційного законодавства.

1.3. Підстави для обробки персональних даних

Український закон визначає[20] перелік підстав для обробки персональних даних:

---

19 Принцип підзвітності, визначений у статті 5 (2) Регламенту, означає, що контролери повинні мати можливість продемонструвати свою відповідність принципам обробки даних.

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

- згода суб'єкта персональних даних;
- дозвіл на обробку персональних даних, який надано відповідно до закону лише для здійснення чітко визначених повноважень;
- укладення та виконання правочину, стороною якого є суб'єкт персональних даних або який укладено на його користь чи для здійснення заходів, що передують укладенню правочину на вимогу суб'єкта персональних даних;
- захист життєво важливих інтересів суб'єкта персональних даних;
- необхідність виконання обов'язку володільця персональних даних, який передбачений законом;
- 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 обробкою його даних переважають такі інтереси.

ОМС є суб'єктом владних повноважень. Відповідно до статті 19 Конституції України ОМС, 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 положення місцева влада може здійснювати обробку персональних даних (будь-яка дія або сукупність дій) лише за наявності повноважень, законної підстави й обґрунтованої мети та у спосіб, передбачений законом.

Тобто не потрібно отримувати згоду суб'єкта персональних даних у тих випадках, коли дозвіл на збір інформації прямо передбачено законом. Водночас недостатньо мати повноваження, має бути обґрунтована мета та чітка процедура.

Підстави «необхідність виконання обов'язку, який передбачений законом» і «необхідність захисту законних інтересів» можуть застосовуватися ОМС для обробки даних лише з певними застереженнями.

Наприклад, місцева влада часто для впровадження систем відеоспостереження обирає підставу «захист життєво важливих інтересів», що некоректно. Під «життєво важливими інтересами» слід розуміти не загальну безпеку громади, а тільки ті інтереси,

які безпосередньо пов'язані з питаннями врятування життя і здоров'я людини. Наприклад, ця підстава актуальна у випадку, коли необхідно отримати персональні дані людини в медичних цілях, а вона не може дати згоду на це через свій безпорадний стан. У міжнародних актах визначені й інші можливості застосування підстави «захист життєво важливих інтересів», коли обробка персональних даних здійснюється для моніторингу розвитку епідемій, під час ліквідації стихійного лиха або катастрофи тощо.

Чому важлива законна основа для обробки?

Обробка персональних даних може здійснюватися тільки законно, справедливо та прозоро. Якщо відсутня законна підстава для збору інформації, тоді така діяльність буде вважатися неправомірною.

Як вирішити, коли застосовується законна підстава?

Це залежить від конкретних цілей і контексту обробки. Водночас досить часто застосовуються декілька підстав, усе залежить від суб'єкта, що збирає інформацію. Але бажано задокументувати таке рішення. Жодна з перелічених основ не може вважатися кращою або важливішою, ніж інші. У законі немає ієрархії в порядку списку.

1.4. Проєктування дизайну приватності

Законодавство у сфері захисту персональних даних вимагає від усіх суб'єктів, що 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 (дизайн приватності) — означає, що особа, яка збирає дані, зобов'язана вбудувати систему їх захисту в усі процеси своєї діяльності ще на ранньому етапі їх проєктування і повинна підтримувати таку систему безперервно й надалі. По суті в законі робиться акцент на превенції всіх можливих ризиків, наприклад витоку даних.

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 імплементовані відповідні технічні та організаційні заходи безпеки інформації. Тут доречно згадати принцип мінімізації даних — що менше даних організація збирає й 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»[21], 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. Але починати роботу потрібно на етапі проєктування, гарантувавши, що всі дані надійно зберігаються, а потім своєчасно знищуються.

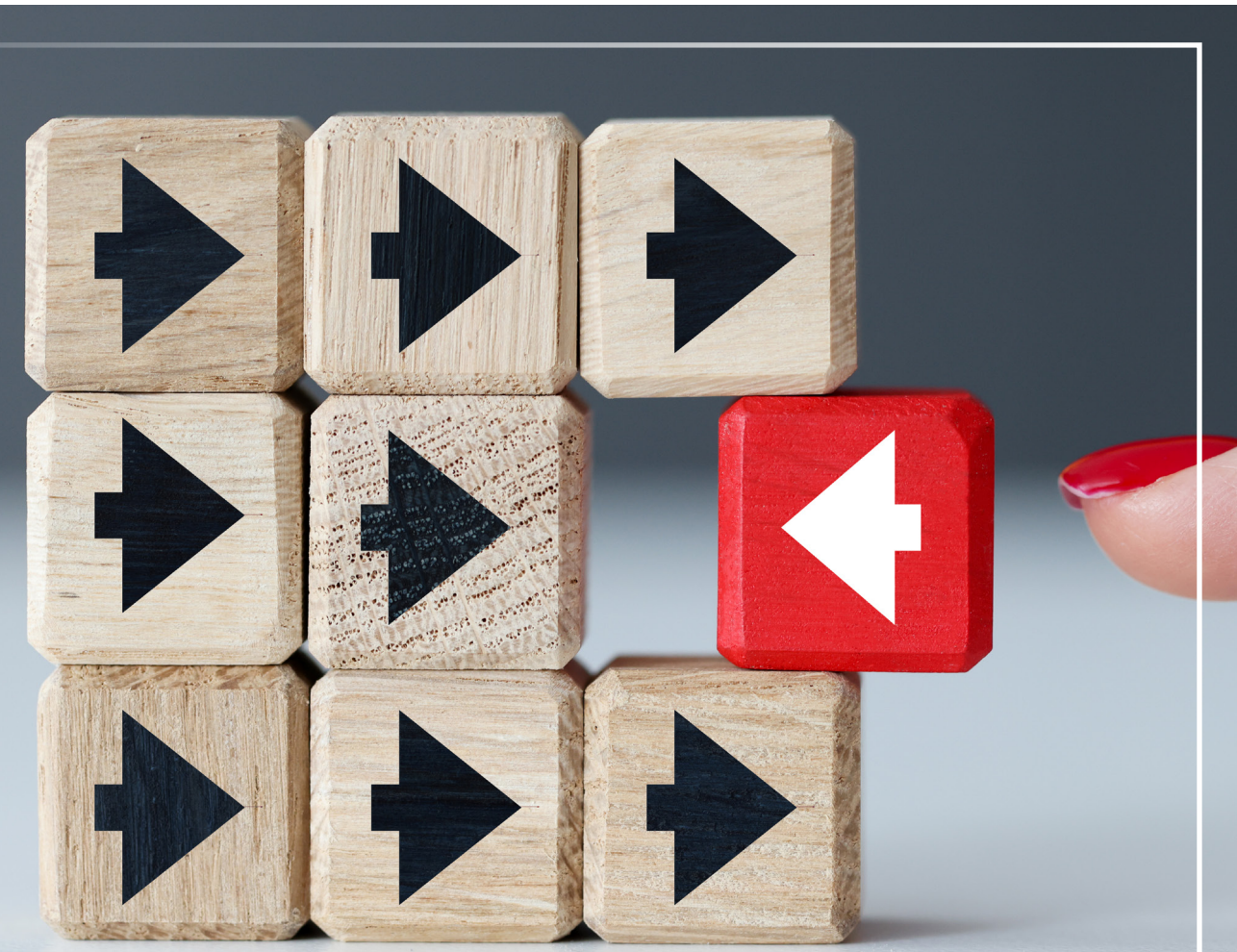
Профілактика, а не лікування. Такий підхід запобігає порушенням приватності до того, як вони відбудуться, оскільки така концепція інтегрується в продукт ще до початку його розробки.

Принципи privacy by design і privacy by default ухвалені більшістю країн як стандарт у сфері захисту персональних 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.

---

21 Ann Cavoukian, Ph.D. Privacy by Design. The 7 Foundational Principles: *https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf*



Розділ 2.

Загальні концепції
управління ризиками

Процес обробки та захисту персональних даних ґрунтується на підході, який передбачає систематичне оцінювання ризиків, які можуть виникнути як для суб'єктів, що їх збирають, так і для осіб, кому вони належать.

Управління ризиками полягає в описі всіх процесів роботи з даними усередині й ззовні (у випадках, якщо дані передаються третім особам) організації. Зокрема, ідеться про пошук найбільш вразливих місць у системі захисту інформації, які допоможуть не допустити помилок у майбутньому.

Може виникнути питання, чи потрібно кожному структурному підрозділу ОМС окремо проводити оцінювання ризиків? Чи це повинна бути єдина загальна процедура для всіх напрямків роботи?

По-перше, ОМС відрізаються за своїм складом. По-друге, з огляду на розгалуженість напрямків роботи органу кожен його структурний підрозділ (або підпорядкована установа) збирає різний вид і категорію персональних даних. Понад те, обробка здійснюється для різних цілей та в різний спосіб. Це означає, що процедуру оцінювання ризиків з питань захисту персональних даних варто здійснювати окремо (наприклад, управління охорони здоров'я й комунальної власності). Водночас хорошою буде вважатися практика, якщо в ОМС затверджено єдиний стандарт здійснення цього процесу.

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

Визначення загального контексту діяльності суб'єкта оцінювання. Для початку потрібно проаналізувати напрямки роботи загалом. Зібрати базову інформацію, яка допоможе зрозуміти, чим займається підрозділ, його напрямки роботи, загальні цілі, команду, локацію, партнерів тощо. Часто на практиці можна почути: треба скласти детальний профіль суб'єкта оцінювання.

Визначення мети. Від мети аналізу буде залежати сценарій і зміст його методології, а також те, скільки треба часу для його проведення, ресурсів і який очікуваний результат. Як каже відома приказка, якщо не знаєш, куди хочеш потрапити, тоді неважливо, якою дорогою йти.

Складання методології. Саме від «профілю суб'єкта оцінювання» та цілей буде залежати завдання та зміст методології.

Аналіз. Коли вже є детальний профіль суб'єкта, визначена ціль та складена методологія аналізу, настає відповідальний етап — безпосереднє оцінювання ризиків.

Стратегії реагування (усунення недоліків). Після того, як ключові проблеми (ризики) зрозумілі, варто подумати про стратегію їх розв'язання та відстеження змін.

Часто оцінювання ризиків сприймають як формальний обов'язок, який треба здійснювати один раз на певний проміжок часу. Насправді це не так, бо підстав для аналізу може бути багато, але про них у наступних розділах.

2.1. Поняття «аналіз ризиків»

Управління ризиками — це не просто абстрактна тема зі світу менеджменту, а необхідний інструмент, який допомагає уникнути негативних наслідків у межах діяльності. Ним часто нехтують, ухвалюючи рішення на основі суб'єктивної думки про потенційні загрози.

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[22].

DPIA — це процес, покликаний допомогти систематично аналізувати, виявляти й мінімізувати ризики для персональних даних під час їх обробки. Це ключова частина зобов'язань щодо підзвітності в діяльності. Неможливо передбачити всі можливі ризики, але можна вжити певні заходи, щоб їх мінімізувати, — саме в цьому суть DPIA.

---

22 «The Practical Guide for Data Protection Impact Assessments subject to the GDPR» published by the AEPD. Standards ISO-29134 «Guidelines for privacy impact assessment», ISO-31000 «Risk management. Principles and guidelines» and ISO-31010 «Risk management. Risk assessment techniques».

Не існує єдиного шаблона, як оцінювати вплив на захист персональних даних. Кожна організація розробляє свій інструмент, адаптований під специфіку її діяльності, проте існують загальні стандарти, про які згадано далі в цьому посібнику.

Важливо зазначити, що в правилах оцінювання ризиків можна натрапити на термін ***PIA***, введений GDPR. Офіційно європейський Регламент говорить про оцінювання впливу на захист даних (DPIA). На практиці, якщо проводиться комплексний аудит діяльності всієї організації, тоді застосовується DPIA, якщо оцінювання конкретної операції обробки — PIA.

- DPIA — відповідає на питання, які ризики для прав людини;
- PIA — відповідає на питання, які ризики для організації.

Отже, оцінювання потрібно розглядати як частину стратегічного менеджменту, що буде впливати на ефективність діяльності установи.

Чому важливо проводити аналіз ризиків?

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

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. Це також гарантує, 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[23]. Невиконання DPIA, коли це необхідно, може призвести до притягнення до відповідальності у вигляді великого штрафу.

Однак оцінювання ризиків — це не просто вправа з дотримання вимог закону, а процес, який дозволяє виявляти й усувати проблеми на ранній стадії. У європейських країнах деякі організації

23 Див. підрозділ 1.4 цього посібника.

застосовують практику консультування для DPIA, тобто дають можливість людям висловити свою думку, як використовується їхня інформація. Також варто подумати й про економічні вигоди, бо, виявивши проблему на ранній стадії, можна зекономити на її розв'язанні.

Трапляються випадки, коли керівники вважають, що вони й без додаткових методологій бачать повну картину всіх процесів й інтуїтивно відчувають потенційні ризики. Проте історія знає багато прикладів, коли можна було уникнути небезпечних ситуацій, якби ними краще управляли.

Коли проводити оцінювання ризиків?

Періодичність оцінювання ризиків буде залежати від специфіки діяльності установи та контексту обробки даних. Аналізувати роботу з даними переважно необхідно у двох випадках: або безпосередньо перед початком збору й обробки даних, або в разі істотних змін у вже чинних процесах. Проведення внутрішнього аналізу не повинно бути складним або вимагати багато часу.

У європейському законодавстві DPIA може передбачати як комплексний аудит діяльності, так і аналіз лише однієї операції обробки даних. Наприклад, пунктом 84 GDPR визначено, що:

> *«...контролер повинен нести відповідальність за проведення оцінювання впливу на захист даних з метою визначення, зокрема, походження, специфіки, особливості та ступеня тяжкості такого ризику. Необхідно враховувати результати оцінювання під час визначення належних заходів, яких необхідно вжити для підтвердження того, що опрацювання персональних даних відповідає цьому Регламенту».*

Іншими словами, законодавець наголошує, що DPIA — це не просто разова формальність, а процес, який має бути інтегрований на постійній основі в повний цикл діяльності організації. Зокрема, якщо вносяться будь-які істотні зміни в те, як і чому обробляються персональні дані, або в обсяг зібраних даних, необхідно показати, що актуальний DPIA оцінює будь-які нові ризики. Якщо — ні, тоді треба переглянути DPIA.

Ризики під час обробки даних умовно можна розділити на кілька типів:

- незаконний доступ до даних;
- несанкціонована зміна даних;
- видалення даних;
- інші дії, що можуть становити загрозу для життя людини.

Звичайно, що їх набагато більше, але ці найпоширеніші. Ризик завжди має причинно-наслідковий зв'язок. Рівень ризику вимірюється залежно від ймовірності його матеріалізації і потенційного впливу. Оцінювання ризику включає розгляд усіх можливих сценаріїв. Як правило, результатом проведення DPIA є зведена таблиця, у якій описані:

- категорії, цілі, обсяги персональних даних, які обробляє організація;
- процеси їх збору та обробки;
- співробітники й підрядники, які беруть участь у процесі;
- виявлені ризики, слабкі місця і можливі загрози;
- заплановані дії в разі порушення приватності.

Оцінювання ризику повинно бути результатом роздумів про наслідки обробки персональних даних.

2.2. Ризики, які необхідно оцінювати

Під поняттям «ризик» часто мається на увазі сценарій, який описує подію, її причини та наслідки та оцінюється з погляду тяжкості та ймовірності.

Наприклад, у статті 35 GDPR ідеться про те, що DPIA має враховувати «ризики для прав і свобод фізичних осіб». Ключовим положенням є пункт 75 GDPR, який пов'язує ризик з концепцією потенційної шкоди для людей:

«Ризик для прав і свобод фізичних осіб, різної ймовірності та тяжкості, може стати результатом опрацювання персональних даних, що може призвести до фізичної, матеріальної та нематеріальної шкоди, зокрема: коли опрацювання може спричинити дискримінацію, крадіжку персональних даних або шахрайство, фінансові

втрати, шкоду репутації, втрату конфіденційності персональних даних, що захищають як особисту таємницю, несанкціоноване скасування використання псевдонімів або будь-яку іншу істотну економічну або соціальну шкоду; коли суб'єкти даних можуть бути позбавлені своїх прав та свобод або можливості здійснювати контроль над своїми персональними даними...»

Таким чином, підхід, заснований на оцінюванні ризику, стосується як майнової, так і немайнової шкоди. Тобто включає будь-який «значний економічний, соціальний або інший збиток». Вплив на суспільство загалом також може бути значущим фактором ризику.

Які типові порушення?

Ризик — це не завжди означає порушення. Переважно мова йде про певні дії, які можуть призвести до негативних наслідків. Проте інколи самі порушення можуть призвести до високих ризиків для прав людини.

Однією з причин такого стану справ є недостатня обізнаність службовців ОМС з міжнародними нормами й стандартами захисту інформації. Посадові особи можуть неповною мірою розуміти, що їх повсякденна робота (надання муніципальних послуг, організація діяльності комунальних підприємств, створення різноманітних реєстрів, ведення журналів тощо) напряму пов'язана зі збором та обробкою персональних даних, а це покладає на них відповідальність за їх належне зберігання й використання.

Можна виділити декілька типових порушень, на які в першу чергу звертають увагу спеціалісти, що проводять оцінювання.

Не забезпечено належний рівень захисту персональних даних. Персональні дані можуть зберігатися на папері, в інформаційних системах або на інших носіях. Це означає, що загрози для витоку персональних даних виникають не лише в разі кібератаки. Оскільки сьогодні майже вся інформація в державному та приватному секторі оцифровується, ризик злому систем значно вищий. Також проблема витоку може бути пов'язана не із зовнішніми факторами, адже часто працівники самі розповсюджують дані.

Не забезпечено безпечні умови обробки спеціальної категорії даних. Спеціальна категорія даних може становити особливі ризики для людини: переслідування, тиск, фізичну небезпеку або порушення інших прав і свобод.

Не розроблено внутрішню документацію, яка регулює всі процедури роботи з даними. Відсутність внутрішньої регуляції всіх процесів може призвести до ризиків — від порушення загального циклу обробки даних до витоку інформації.

Відсутність процесу видалення даних. Досить часто накопичується надлишковий обсяг інформації, який вчасно ніхто не видаляє. Це можна порівняти із шафою, заповненою непотрібними речами, наявність яких уже ніхто не контролює.

Агрегація даних. Об'єднання різних баз даних завжди становить ризики як для організації внутрішнього менеджменту, бо унеможливлює виконання вимог закону (наприклад, диференціації інформації або вчасного видалення даних), так і людини, чия інформація там міститься, бо таким чином складається її загальний профайл.

2.3. Індикатори, які визначають ступінь ризику

Закон не встановлює чіткої процедури оцінювання ризиків, але визначає, що це потрібно обов'язково робити, якщо тип обробки становить високий ризик[24].

Наприклад, відповідно до статті 29 GDPR особа, що першочергово збирає дані (контролер), встановлює відповідні інструкції щодо їх обробки та захисту. Робоча група органів ЄС у сфері захисту персональних даних опублікувала[25] керівні принципи з критеріями, які можуть виступати як індикатори обробки з високим ступенем ризику:

- автоматизоване ухвалення рішень, що може призвести до негативних наслідків;

---

24 Див. далі, який тип обробки може становити високий ризик.

25 Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01): *https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236*

- дані, що обробляються у великих масштабах;
- зіставлення або об'єднання наборів даних (агрегація баз даних);
- особливі категорії даних;
- використання нових технологій або інших організаційних рішень;
- запобігання використанню суб'єктами даних права або використання послуги або контракту та інше.

У більшості випадків поєднання двох з цих факторів указує на необхідність оцінювання ризиків. Однак не можна сказати, що це суворе правило. Щоразу потрібно самостійно обґрунтовувати своє рішення, коли необхідно аналізувати свою діяльність.

Що може призвести до високого ризику?

Європейське законодавство (GDPR) вимагає[26] від наглядових органів публікувати список операцій обробки, що потребують DPIA. Це означає, що закон не містить точного опису випадків, коли існує підвищений ризик. При цьому слід звернути увагу на такі моменти:

- Чи використовуються при обробці нові технології?
- Характер обробки.
- Масштаб обробки (тривалість, кількість різних даних, кількість суб'єктів даних).
- Контекст обробки.
- Мета обробки.

З огляду на ці фактори потрібно подумати, чи пов'язана обробка в конкретному структурному підрозділі ОМС з підвищеним ризиком для прав суб'єктів персональних даних. Наприклад, коли:

- обробка персональних даних здійснюється з використанням інноваційних технологій, зокрема штучного інтелекту (AI);
- застосовується автоматизоване ухвалення рішень, включаючи профілювання або обробку даних спеціальної категорії.

Наприклад, автоматичне визначення того, чи має право людина на субсидію, кредит (або іншу виплату) тощо. Особисті

26 Стаття 35 (4) Регламенту.

дані такої особи обробляються за допомогою певного програмного забезпечення, яке в результаті ухвалює рішення: давати кошти чи ні.

1. Застосування масштабного профілювання людей.
2. Обробка медичних, біометричних або генетичних даних, окрім випадків, коли це здійснюється медичними працівниками для надання допомоги людині.
3. Об'єднання, порівняння або зіставлення особистих даних, отриманих з декількох джерел.
4. Обробка, яка включає відстеження геолокації або поведінки людини, включаючи, зокрема, онлайн-середовище.
5. Обробка даних про дитину або інших вразливих осіб у маркетингових цілях, профілюванні або іншому автоматизованому ухваленні рішень.
6. Обробка має такий характер, що витік інформації становитиме загрозу для здоров'я або безпеки людей[27].
7. Робота ОМС в оборонній сфері.

Приклади операцій з обробки персональних даних, що можуть призвести до високого ризику[28]. Цей список не є вичерпним.

Тип обробки	Опис	Приклади наявних сфер застосування
Технології	Обробка, що включає використання нових технологій, зокрема штучного інтелекту (AI).	Штучний інтелект, машинне навчання, робототехніка, інтелектуальні транспортні системи. Маркетингові дослідження з використанням нейровиміру (наприклад, аналіз емоційної реакції й активності мозку тощо).

27 Приклади операцій, що вимагають DPIA, критеріїв високого ризику в поєднанні з іншими, що можуть призвести до високого ризику: *https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/examples-of-processing-likely-to-result-in-high-risk/*

28 Відповідно до рекомендацій, ухвалених Європейською Радою з питань захисту даних, «Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01)».

Автоматичне ухвалення рішення	Автоматичне ухвалення рішень може вплинути або обмежити права і свободи людини.	Наприклад, коли людина отримує продукт чи послугу, кредит, лізинг.
Профілювання	Будь-яке великомасштабне профілювання людей.	Аналіз набору даних для створення таргетингової реклами, політичної агітації тощо.
Біометричні дані	Будь-яка обробка біометричних даних з метою однозначної ідентифікації людини.	Розпізнавання осіб у системах спостереження. Ідентифікація особи для доступу на робоче місце / перевірка особи (за допомогою голосу / відбитків пальців / розпізнавання рис обличчя).
Генетичні дані	Будь-яка обробка генетичних даних, окрім тих, які обробляються для надання екстреної медичної допомоги безпосередньо суб'єкту даних.	Медичний діагноз, ДНК-тестування, медичні дослідження.
Відстежування	Обробка, яка включає відстеження геолокації або поведінки людини, зокрема в онлайн-середовищі.	Соціальні мережі інші програмні, мобільні додатки для аналізу способу життя / здоров'я людини. Або відстежування геолокації для служб таксі. Онлайн-реклама.
Обробка даних дітей / інших вразливих осіб	Використання особистих даних дітей у маркетингових цілях, профілюванні або іншому автоматизованому ухваленні рішень.	Соціальні мережі. Мобільні додатки, онлайн-послуги, що надаються безпосередньо дітям (або недієздатним особам).

Що означає «інноваційні технології»?

Це одне з найбільш дискусійних питань серед юристів з цифрового права. Наприклад, сучасний електрочайник з функцією розпізнання якості води також можна назвати інновацією. Якщо організація має такий пристрій, тоді чи повинна вона проводити оцінювання ризиків?

Відповідь скоріше буде негативною, бо така технологія не передбачає збір й обробку персональних даних.

Наприклад, китайська компанія Taigusys розробила технологію розпізнавання емоцій людини через камери спостереження. На її сайті зазначено, що система допомагає «справлятися з новими викликами» й «мінімізувати конфлікти». Алгоритм зчитує рух мімічних м'язів людини, біометричні сигнали й оцінює їх за індикаторами «позитивних» і «негативних» емоцій. Система може навіть визначати фальшиву усмішку. Розумні камери встановлюють у в'язницях, щоб контролювати ув'язнених і розпізнавати «небезпечну поведінку», на вулицях, у навчальних закладах тощо. Правозахисники виступають проти такого підходу, оскільки вбачають використання біометричних даних людини проти її волі. Від стеження неможливо сховатися. Одна справа, коли подібні пристрої застосовує приватна компанія для моніторингу працівників, які завчасно погодилися на такі умови роботи, а інша — коли держава для контролю суспільства[29].

Цей приклад показує, що технології не стоять на місці, постійно розвиваються. Компанії-розробники демонструють їх переваги, які можуть зацікавити владу. Але за відсутності сталих процесів оцінювання ризиків у впровадженні будь-якої інновації вони можуть призвести до негативних наслідків як для людини, так і населення загалом.

Приклади обробки з використанням інноваційних технологій включають:

- штучний інтелект, машинне навчання;
- автономні та інтелектуальні транспортні системи;
- робототехніку;
- маркетингові дослідження, наприклад з використанням аналізу поведінкових даних людини, емоційної реакції тощо.

---

29 «Forget the Facebook leak»: China is mining data directly from workers' brains on an industrial scale: *https://www.scmp.com/news/china/society/article/2143899/forget-facebook-leak-china-mining-data-directly-workers-brains*

Використання таких технологій може призвести до високих ризиків для прав і свобод окремої людини та національної безпеки загалом[30].

Наприклад, ОМС вирішить оснастити громадський транспорт функціями відстеження геолокації, що дозволить у будь-який час знати маршрут пересування водіїв. У цьому випадку може виникнути дисбаланс між правом знати розташування транспорту й приватним життям співробітників. Тому для цього проєкту також варто проводити оцінювання ризиків ймовірних порушень прав і свобод людини.

Що означає «істотний вплив»?

Український і європейський закони конкретно не визначають цього поняття. Проте в керівних принципах статті 29 GDPR у контексті положень про профілювання є деякі додаткові вказівки. Одним словом, істотний вплив — це те, що може вплинути на поведінку людини та спонукати її до певних дій.

Наприклад, соціальні мережі використовують мікротаргетинг для ідентифікації певного типу людей, щоб потім цілеспрямовано направляти їм потрібну інформацію для формування певного переконання. Уже існує багато механізмів, щоб визначити, яка картинка або повідомлення подобаються конкретним особам чи навпаки викликають негативні емоції, що саме змусить їх проголосувати за політичну силу, підтримати ідею й т. д.

Також значний ефект може включати щось, що впливає на фінансове становище, здоров'я, репутацію, доступ до послуг або інші

економічні або соціальні можливості людини. Зокрема рішення, які можуть вплинути на більш вразливих людей, наприклад дітей[31].

---

30 Більше про великі дані, штучний інтелект, машинне навчання в матеріалі, що містить додаткові інструкції із застосування цих технологій у контексті захисту даних: *https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf*

31 Керівництво WP29 з автоматизованого ухвалення рішень і профілювання для цілей Регламенту 2016/679 (WP251).

Що означає «вразливість»?

Вразливість в інформаційному середовищі не означає, що людина має фізичні вади, асоціальний статус або певний вік. Тут скоріше мова йде про спроможність будь-якої людини контролювати процес обробки своїх даних та усвідомлювати можливі наслідки. Найбільш очевидно, що діти або недієздатні особи вважаються вразливими, бо вони можуть не розуміти, як їхні персональні дані використовуються, і захистити себе від будь-яких небажаних ризиків.

Що означає «масштабна обробка»?

Для того, щоб вирішити, чи є обробка масштабною, треба враховувати:

- обсяг і різноманітність даних, що обробляються;
- кількість осіб, чиї дані обробляються;
- географічне охоплення обробки.

Наприклад, масштабну обробку даних ОМС здійснюють під час застосування апаратних комплексів систем відеоспостереження; страхова компанія або банк, що обробляє дані клієнтів; пошукова система, що обробляє поведінкові дані для таргетингової реклами; або провайдер інтернет-послуг, що обробляє дані користувачів тощо.

2.4. Етичні принципи під час застосування цифрових технологій

У 2020—2021 роках у світі набули неабиякої популярності теми, пов'язані з незаконною обробкою персональних даних, стеженням, кібершахрайством і нерівним доступом до розвитку технологій.

Уряди різних країн приділяють велику увагу питанням етики під час застосування цифрових технологій, особливо в державному управлінні. Створено чимало документів, керівництв і кодексів, а також напрацьовано практику їх використання. Велика Британія — один з найкращих прикладів методичного забезпечення в цій сфері. На державному порталі gov.uk опубліковано Керівництво з етичного використання даних в органах влади та державному

секторі загалом[32]. Воно містить загальні етичні принципи (зокрема, відкритість, відповідальність, чесність) роботи з даними. Для кожного принципу наведені конкретні кроки з реалізації на практиці.

При федеральному уряді Німеччини працює Комісія з етики даних[33], завдання якої — розробка етичних принципів для захисту особи, збереження єдності суспільства й розвитку інформаційних технологій. Наприклад, у 2020 році в ЄС запропонували запровадити так звані «паспорти імунітету» як спосіб доводити, що в людини є антитіла до COVID-19. Деякі українські чиновники також висловилися на підтримку цієї ідеї, бо це дозволить безпечно подорожувати або повертатися на роботу. Така ініціатива спричинила бурхливу дискусію серед громадськості. У Німеччині вирішили детальніше в цьому розібратися, перед тим як ухвалювати рішення. Німецьке міністерство охорони здоров'я звернулося до Ради з питань етики, яка згодом опублікувала свій висновок, де не рекомендувала впроваджувати такі заходи. Серед аргументів було те, що у світі ще немає чітких даних про ефективну превенцію від захворювання. Жодне дослідження не довело, що антитіла до SARS-CoV-2 захищають від повторного інфікування. Термін дії паспорта має бути обмежений, а значить необхідно повторно проходити обстеження. По суті людині потрібно буде постійно доводити, що вона не хвора, розкриваючи широкому колу інформацію про стан свого здоров'я. Німецькі експерти зробили висновок, що такий тиск з боку держави або роботодавців є надмірним і може негативно вплинути на вразливі групи. До того ж необхідна відповідна законодавча база, яка регулюватиме процедури використання документа, створення баз даних і порядку їх обробки[34]. Тобто «паспорти вакцинації» повинні видаватися за добровільною згодою особи.

Цифрова трансформація в Україні також потребує своєчасних відповідей на етичні питання, що виникають при використанні цифрових технологій, у міру того, як вони змінюють стиль державного управління та роль службовців загалом.

---

32 Data Ethics Framework: *https://www.gov.uk/government/publications/data-ethics-framework/data-ethics-framework-2020*

33 Datenethikkommission: *https://www.bmjv.de/DE/Themen/FokusThemen/Datenethikkommission/Datenethikkommission_EN_node.html*

34 «Immunity passports» in the context of COVID-19: *https://perma.cc/9KEZ-SPHX*

Можемо спостерігати, що в нових умовах службовцям у процесі ухвалення рішень усе більше доводиться покладатися на персональну відповідальність, тоді як раніше вони могли чітко дотримуватися встановленого регламенту. Найбільш це відчувається саме при застосуванні інформаційного законодавства. Наприклад, у 2011 році набув чинності Закон України «Про доступ до публічної інформації», тоді за своєю суттю цей акт став фактично революційним, бо на відміну від інших вимагав від чиновників самостійно ухвалювати рішення, коли можна надавати публічну інформацію, а коли — ні. Зокрема, визначати баланс між правом суспільства «знати» й захистом даних. З'явилося таке поняття, як трискладовий тест, за допомогою якого треба аналізувати кожен окремий випадок надання інформації та оцінювати ризики від ухваленого рішення. Саме тоді, хоч не дуже широко, заговорили про етичні принципи як правила поведінки, які критично впливають на рівень довіри громадян до держави, а в перспективі — на її стабільність і розвиток.

Звичайно, на питання формування довіри суспільства до технологій потрібно дивитися ширше, ніж просто на роботу конкретної установи. З кожним роком оптимізм щодо цифрового майбутнього згасає, бо люди все більше відчувають на собі ризики для своїх прав та свобод. В результаті це призводить до індивідуального спротиву або взагалі до загального протестного руху. Яскравий приклад — протидія бажанню муніципалітетів встановлювати системи розпізнання обличчя, зокрема надавати прямий доступ до баз даних органам правопорядку. Усе це доповнюється скандальними ситуаціями масштабних витоків персональних даних та використання їх у небросовісних цілях. У міру того, як інноваційні технології стають повсякденністю в економіці, обороні, охороні здоров'я, у відносинах людини з державою, ризиків стає все більше.

Очевидно, що технологічні прориви останніх десятиліть готували ґрунт для того, що сьогодні значна частина життя людини реалізується в мережі. Найцікавіше, що серед ключових ініціаторів цифрової трансформації є саме держава, яка активно просуває нову модель — «безконтактної економіки», а також правоохоронної діяльності. Пандемія значно вплинула на ухвалені в цей період управлінські рішення у сфері цифровізації.

З одного боку, така ситуація принесла користь. Наприклад, місцеве самоврядування побачило, як можна оптимізувати свою роботу за допомогою технологій, не роздувати штат, задовільняти потреби суспільства дистанційно. Окремі чиновники заговорили про те, що будуть збирати масиви даних для аналізу й навчання систем штучного інтелекту (AI), сприяючи розвитку цифрової медицини, правоохоронної діяльності та охорони навколишнього середовища у своєму регіоні. Скажімо, екологи отримають можливість ефективніше аналізувати ситуацію із забрудненням повітря, працівники комунальних підприємств — удосконалити роботу транспортних систем тощо.

З іншого боку, недостатньо побачити переваги, потрібно також навчитися добре розуміти ризики. Непродумані рішення можуть завдати значну, інколи непоправну шкоду як людині, так і громаді. Замість зміцнення довіри суспільства до діяльності установи, навпаки, отримати супротив. У цьому контексті можна навести приклад, коли під час локдауну окремі представники місцевої влади пропонували соціальний моніторинг і контроль пересування населення. Надмірне втручання в приватне життя людини та тотальний збір її персональних даних спричинили неабияке занепокоєння в суспільстві. Аспектами нової реальності стали безпрецедентний доступ і використання особистих даних людини. Якщо раніше збір даних за допомогою технічних засобів вимагав процедур у межах оперативно-розшукової діяльності, то сьогодні технології стеження розвивають і муніципалітети.

Одним словом, етичні питання щодо роботи з інформацією про людину, яким раніше не приділяли увагу, стають дедалі вразливішими в процесі диджиталізації. Сьогодні при розробці та впровадженні муніципальних сервісів рішення ухвалюються переважно інтуїтивно. Тоді як обсяги персональних даних, які постійно зростають, вимагають прикладного регулювання та встановлення чітких правил і принципів[35].

Процес обробки персональних даних потребує нових підходів, зокрема підвищення цифрової грамотності як держслужбовців, так і населення загалом. Окремі норми ділової етики службовця

35 Ethical principles of the use of data: https://www.analyticsinsight.net/ethical-principles-for-using-data/

затверджені низкою законів. Окрім того, в органах влади, ОМС можуть бути спеціальні внутрішні етичні кодекси. Однак нормативів, які регламентували б діяльність в умовах цифрової трансформації для держслужби, поки немає.

З огляду на події та реакції громадськості на просування технологічних рішень уже скоро державним і місцевих органам влади буде критично важливо мати зрозумілі етичні принципи ухвалення своїх рішень. Довіра з боку громадськості буде танути, якщо технології використовуються неетично або коли їх застосування породжує страх та завдає шкоду людям.

Є декілька аспектів, що посилюють значущість етичних питань у цифровому середовищі. По-перше, створення онлайн-послуг, які фундаментально змінюють підхід до відносин між суб'єктами владних повноважень і людиною. Наприклад, нові форми спілкування — чат-боти замість людей тощо. По-друге, технологічні рішення, які впливають на поведінку, життя й здоров'я людини. Зокрема, застосування програм з вбудованим штучним інтелектом і роботизацією, що, між іншим, ще не врегульовано законом. І наостанок, відсутність ефективних практик оцінювання ризиків при запровадженні нових технологій. Коли місцева влада говорить про переваги сучасних послуг, вона не завжди готова говорити про ймовірні наслідки. Ідеальних рішень не існує, але в кожному разі суспільству потрібно чесно говорити, хто в цій історії виграє, а хто може програти, уміти обґрунтувати логіку своїх дій, мати відповіді на складні питання. Якщо ж влада не може цього пояснити, уникає відповідальності, посилаючись лише на абстрактні судження, тоді можна дійти висновку, що насправді ситуація не під контролем і все ж таки існують загрози.

У процесі ухвалення рішення треба аналізувати, чи присутня в ньому етична складова. Не треба боятися виносити етичні проблеми на обговорення, аналізувати їх і стежити за світовою практикою.

В ідеальній картині світу держава повинна захищати інтереси, права й свободи людини. Багато ситуацій, які щодня виникають у цих взаємовідносинах, потребують балансу інтересів. Коли суспільству будуть чітко зрозумілі етичні принципи, якими керується окремий службовець, ухвалюючи рішення, це буде зменшувати

напругу й посилюватиме довіру. Відсутність системної роботи з ризиками може призводити до недостатньо продуманих рішень. Зокрема, ідеться про випадки, коли робиться акцент на майбутніх позитивних ефектах і недостатньо враховуються потенційні негативні.

Дизайн цифрового рішення (сервісу або послуги) повинен бути інклюзивним і враховувати особливості різних груп користувачів. Багато інтерфейсів розроблені для людей з хорошим зором і моторикою, але не враховують інтереси сліпих і глухонімих. Інклюзивність послуг — це не тільки про встановлення пандусів або збільшення шрифту на вебсайті, це передусім про можливість враховувати потреби всіх без винятку людей. Така концепція має бути фундаментальною при розробці інноваційних рішень. Якщо інструмент передбачає ухвалення персоналізованих рішень про надання послуг або застосування санкцій (наприклад, у разі порушення правил паркування авто), то вони повинні відповідати вимогам законності та справедливості[36].

Наслідки взаємодії із цифровим інструментом або сервісом повинні бути передбачувані.

Отже, перед тим, як запровадити новий цифровий сервіс або інше рішення, варто використовувати інструменти (фреймворки або чеклісти), які допомагають оцінювати ризики, пов'язані з дизайном і параметрами його роботи[37]. Наприклад, серед питань, які варто включити:

- Яку користь принесе цифрове рішення тим, хто буде ним користуватися, і суспільству (громаді) загалом?
- Чи є групи людей, яким цифрове рішення може нашкодити?
- Чи можна виміряти користь або ймовірну шкоду, яку принесе цифрове рішення?
- Чи є групи людей, які не отримають від цифрового рішення жодної користі?
- Які технічні рішення (програми) будуть використовуватися?

---

36 Data Ethics Principles: https://dataethics.eu/data-ethics-principles/

37 При розробці фреймворку можна використати Data Ethics Canvas — графічний інструмент для етичної роботи з даними, розроблений Відкритим інститутом даних.

- Чому обрали саме ці рішення (програми)?
- Чи мали ці рішення в минулому інциденти, пов'язані з витоками даних або іншими порушеннями у сфері приватності?
- Яким чином буде здійснюватися контроль у сфері захисту інформації?
- Чи достатньо поінформоване суспільство про суть, мету проєкту (цифрового рішення) і хід його реалізації?
- Чи достатньо поінформоване суспільство, для чого будуть збиратися та використовуватися персональні дані?
- Чи достатньо поінформоване суспільство про роботу технології та можливі ризики?
- Чи забезпечено громадське обговорення та чи люди мали змогу висловити свою думку або заперечення?
- Чи може призвести розробка цифрового рішення до обмеження законних прав та інтересів людей або організацій?
- Як таке рішення сприятиме розширенню прав і можливостей людини, зокрема зменшенню економічної, соціальної, гендерної нерівності тощо?
- Чи вплине цифрове рішення на навколишнє середовище?
- Чи використовується в цифровому рішенні штучний інтелект, який його вплив?
- Чи можна досягти цілей проєкту, використовуючи менший обсяг даних?
- Чи відповідає порядок збору й обробки даних вимогам законодавства?
- Чи може цифрове рішення викликати занепокоєння в суспільстві й чому?
- Чи визначена категорія критичних ризиків?
- Чи є стратегія управління ризиками?
- Чи є план заходів зі зниження ризиків?[38]

38 Data Ethics Framework — фреймворк британського уряду для етичної роботи з даними й розробки цифрових рішень.

Розділ 3.

Проведення аналізу ризиків

Управління ризиками передбачає скоординовані заходи з аналізу ситуацій, які можуть призвести до витоку даних або інших інцидентів інформаційної безпеки. Якщо ОМС уже має власну політику оцінювання ризиків, її потрібно періодично переглядати, щоб вона була актуальною та відповідала положенням законодавства.

Якщо ОМС не має розроблених процедур оцінювання ризиків, їх потрібно впроваджувати у свою діяльність. Можна використати шаблони, які пропонують контролюючі органи або експерти. Така практика цілком прийнятна. Понад те, вона додає впевненості, що в аналізі будуть враховані всі необхідні аспекти у сфері захисту персональних даних.

Водночас, якщо специфіка діяльності підрозділу (або підпорядкованої установи) потребує постійного оцінювання ризиків, оскільки він здійснює обробку даних, що становлять особливий ризик, краще розробити індивідуальну методологію, яка буде відповідати його конкретним потребам.

Наприклад, ОМС встановлюють системи відеоспостереження. За допомогою відеозапису можна прямо чи опосередковано ідентифікувати особу за фізіологічними та зовнішніми ознаками — рисами обличчя, кольором волосся, параметрами тіла, голосом тощо. Понад те, збирається категорія даних, які можуть становити особливий ризик для людини. Упізнання особи під час перебування на мирних зібраннях може вказувати на її політичні вподобання; зафіксовані на відео візити до певного медичного закладу — свідчити про стан здоров'я; відвідування культових споруд — про ті чи інші релігійні переконання, а одягнена уніформа — про рід професійної діяльності.

Очевидно, що в загальному діапазоні інформації про людину сегмент даних, які належать до персональних, є великим, а отже, і вразливим для широкого спектра ризиків.

3.1. Ключові кроки процесу аналізу ризиків

Немає єдиного сценарію проведення оцінювання ризиків у сфері захисту персональних даних, але з огляду на практику варто передбачити такі кроки:

- **Крок 1:** сформувати команду та визначити ціль, для чого проводити

оцінювання ризиків (наприклад, початок нового проєкту або систематична робота).

- Крок 2: визначити процеси обробки, що підлягають оцінюванню (наприклад, збір, реєстрація, поширення інформації або все разом, тобто повний цикл обробки).
- Крок 3: провести консультації з різними сторонами як з питань можливих ризиків, так і процесу їх оцінювання загалом.
- Крок 4: виявити та оцінити ризики.
- Крок 5: перевірити виконання зобов'язань особами (юридичними або фізичними), яким передаються дані.
- Крок 6: визначити заходи зі зниження ризиків.
- Крок 7: описати результати та інтегрувати їх у діяльність.

Крок 1. Формування команди, визначення цілей та очікуваних результатів

Оцінювати ризики варто на різних етапах будь-якої роботи з персональними даними. Саме тому важливо запровадити практику формування дизайну приватності (privacy by design)[39] на постійній основі, залучаючи різних спеціалістів, які будуть брати участь у цьому процесі: менеджерів, інженерів, персонал з питань інформаційної безпеки, юристів тощо.

Перед тим, як розпочати розробляти методологію та проводити оцінювання ризиків, важливо визначити конкретні цілі та результати. Тобто відповісти на питання: для чого це потрібно робити?

Якщо мова йде про розробку нового продукту або послуги[40], тоді краще оцінювати повний життєвий цикл обробки даних (наприклад, у межах діяльності структурного підрозділу ОМС запускається новий проєкт, напрям роботи або послуга для населення). Якщо питання стосується ризиків на конкретному етапі (скажімо, треба зрозуміти, чи є ризики під час передачі конфіденційної інформації третім особам), тоді цілі та зміст методології будуть формуватися на основі конкретної потреби.

---

39 Детальніше у підрозділі 1.4 цього посібника.

40 Процес обробки з повним життєвим циклом функціонування даних: від збору до видалення.

Крок 2. Опис процесів обробки даних

Обробка — це все те, що відбувається з персональними даними. Тому першим і необхідним етапом у процесі оцінювання ризиків є визначення та опис того, на якій підставі, як і чому збирається конфіденційна інформація.

Незалежно від того, наскільки детальною буде розроблена методологія оцінювання ризиків (у тому числі DPIA), важливо зрозуміти базовий контекст роботи з інформацією, яка містить персональні дані.

Наприклад, форма, яка описує цикл обробки даних, може виглядати так:

№	Питання	Відповідь
1.	Які дані збираються (вид і категорія)?	
2.	Чи збираються дані, що становлять особливий ризик?	
3.	З якою метою?	
4.	Яка законна підстава?	
5.	Які джерела збору?	
6.	Де реєструються?	
7.	Де накопичуються та зберігаються?	
8.	Який термін зберігання?	
9.	Чи змінювалися дані?	
10.	Як використовуються?	
11.	Чи використовуються інноваційні технології?	
12.	Чи використовуються нові типи обробки інформації?	
13.	У кого є доступ до даних (підстава та умови)?	
14.	Чи поширюються дані та яким чином?	
15.	Чи передавалися третім особам? На якій підставі та у який спосіб?	
16.	Чи передавалися розпорядникам? На яких умовах та у який спосіб?	
17.	Чи знеособлюються дані? Якщо так, тоді дані яких категорій?	
18.	Які заходи безпеки даних?	
19.	Які способи видалення даних?	

Відповіді на ці питання дозволяють створити «профіль» конкретного структурного підрозділу (установи) і надалі розробляти детальні, адаптовані методології для оцінювання ризиків і впливу на захист даних.

Контекст обробки — це більш широка картина, включаючи внутрішні й зовнішні чинники, що мають значення для захисту даних. Наприклад:

- джерело збору даних (наприклад, окрім встановлених внутрішніми правилами джерел отримання інформації, можуть з'являтися додаткові, які також потрібно врахувати. Серед поширених випадків: за допомогою власних мобільних пристроїв, персональних комп'ютерів, додаткових програм, які раніше не використовувалися тощо);
- здатність людей контролювати свої дані (наскільки забезпечується право людини на інформацію та принцип прозорості діяльності в цій сфері);
- категорії осіб (наприклад, чи є серед них діти, резиденти інших країн);
- технології, що застосовуються для обробки даних;
- актуальні питання, що спричиняють занепокоєння в суспільстві (поширені приклади: встановлення систем відеонагляду, робота в оборонній галузі, сфері охорони здоров'я та соціального захисту населення);
- чи дотримується організація яких-небудь кодексів / правил поведінки у сфері захисту даних або чи пройшла процедури сертифікації на відповідність міжнародним стандартам ISO та ін.

Аналіз реєстрів обробки даних

Обробка персональних даних проходить певний життєвий цикл — від збору до видалення. Тобто залежно від мети збору кожен вид інформації передбачає свій сценарій обробки. Одні дані збираються тільки для збереження, а інші для подальшої передачі або поширення. Тому варто обрати реєстри даних для аналізу та визначити найвищі ризики як для людини, чиї дані збираються, так і для організації загалом.

Наприклад, це можна зробити, застосувавши шкалу вірогідності. Складаємо всі реєстри (бази) обробки даних, а потім для кожного

окремо оцінюємо ризики. Далі робимо диференціацію за ступенем загрози. Першими будуть ті, що мають найвищий вплив.

Крок 3. Консультації

Важлива частина процесу оцінювання ризиків, яку не варто недооцінювати, — це проведення консультацій з різними сторонами: командою проєкту, експертами у сфері захисту персональних даних, партнерськими організаціями (розпорядниками даних), а також контролюючим органом[41]. Погляд зі сторони — важливий. Варто документувати думки окремих осіб і в разі потреби отримати офіційне роз'яснення від державних органів, що дотичні до цієї сфери.

Цей етап не є обов'язковою частиною процесу оцінювання ризиків, проте з юридичного погляду може стати дуже важливим аргументом у разі виникнення суперечливих ситуацій у ході діяльності з обробки даних.

Водночас хорошою вважається практика, коли питають думку самих суб'єктів персональних даних. Наприклад, які загрози вони бачать у контексті обробки їх особистої інформації. Можливо, отримані відомості не стануть підґрунтям для розробки якісної методології, але точно підвищать довіру до установи. Для цього слід розробити процес консультацій, за допомогою яких дізнатися бачення різних сторін. Зокрема, тих, хто відповідає за інформаційну безпеку. Якщо на якомусь етапі погляди будуть відрізнятися, тоді варто зафіксувати їх, а також причини[42].

Крок 4. Виявлення та оцінювання ризиків

Під час оцінювання ризиків для людини, що можуть настати в результаті обробки даних, варто звернути увагу на:

- порушення, зокрема, права на недоторканність приватного життя;

---

41 Якщо організація здійснює свою діяльність на території ЄС, тоді згідно зі статтею 36 GDPR вона повинна провести попередні консультації. В Україні парламентський контроль у сфері захисту персональних даних здійснює Уповноважений Верховної Ради України з прав людини.

42 Some SAs such as the ICO have DPIA guidance with a section on consultation: *https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-dataprotection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-do-adpia/#how7*.

- втрату контролю над використанням персональних даних;
- можливу дискримінацію;
- загрози кібербезпеці (онлайн-шахрайство тощо);
- репутаційні ризики;
- будь-який інший значний економічний або соціальний збиток.

Під час оцінювання ризиків варто описувати кожен процес обробки даних окремо (наприклад, окремо збір, реєстрацію, використання, поширення, передачу тощо). Це дозволить врахувати ступінь ризику, причини його настання та наслідки на кожному етапі загального циклу функціонування конфіденційної інформації. Можна скористатися структурованою матрицею:

Назва процесу обробки даних	Вид і категорія даних (також, можливо, ще категорії осіб, чиї дані	Опис процесу (джерела, спосіб, місце, час тощо)	Рівень впливу на захист даних	Ймовірність виникнення шкоди	
				Рівень ризику	Обґрунтування ризиків
Наприклад, збір даних	Наприклад, ПІБ, електронна адреса, номер телефону	Наприклад, за допомогою реєстраційної форми на вебсайті	Серйозний вплив	Низький ризик	Усі можливі ризики, їх причини та наслідки
	Підпис, ПІБ, номер телефону, паспортні дані, адреса місця проживання, ідентифікаційний код	Особисті зустрічі	Середній вплив	Середній ризик	
	Підпис і ПІБ	Під час заповнення реєстраційних карток	Мінімальний вплав	Високий ризик	

Наведена вище матриця може доповнюватися різними питаннями, які стосуються роботи з інформацією[43]. Головне досягнути очікуваного результату — максимально якісно оцінити всі можливі ризики або порушення.

Наприклад, ще часто використовують систему оцінювання через виставлення балів. У такий спосіб можна оцінити й внутрішні ризики — втрату репутації, суспільної довіри, ресурсів, економічної вигоди тощо.

Крок 5. Перевірка виконання зобов'язань особами, яким передаються дані

Якщо установа передає (зокрема, за договором) персональні дані розпоряднику, це потрібно взяти до уваги в процедурі оцінювання ризиків. У договорі повинні бути описані всі процедури роботи з конфіденційною інформацією та умови її захисту. Тому під час оцінювання ризиків варто перевірити умови співпраці та зобов'язання. Наприклад, такий договір повинен включати:

- предмет, характер і мету обробки даних;
- тривалість обробки;
- вид і категорію персональних даних;
- категорії суб'єктів даних;
- обов'язки і права організації-володільця даних;
- зобов'язання щодо виконання вимог (інструкцій) порядку обробки та захисту даних;
- порядок та умови доступу до даних на вимогу третіх осіб;
- процедури збереження та видалення даних.

Крок 6. Визначення заходів зі зниження ризиків

Просто виявити ризик — недостатньо. Потрібно визначити джерело, причину виникнення та ймовірні наслідки кожного з них. Це дозволить розглянути варіанти того, як знизити конкретний ризик. Наприклад, такі:

- рішення не збирати певні типи даних;
- скорочення обсягу обробки;

43 Зокрема тими, що передбачені кроком 2 «Опис процесів обробки даних».

- скорочення термінів зберігання даних;
- вжиття додаткових заходів технічної безпеки;
- залучення додаткових спеціалістів управління даними;
- анонімізація або псевдонімізація даних, де це можливо;
- розробка додаткових внутрішніх інструкцій і політик;
- використання іншої технології;
- підвищення кваліфікації персоналу в цій сфері;
- посилення заходів контролю та інше.

Це не вичерпний список. Кількість способів уникнути ризиків прирівнюється до ймовірності їх виникнення.

Крок 7. Опис результатів та їх інтеграція у діяльність

Після того, як визначені ризики, ймовірні джерела виникнення, причини та наслідки, слід узагальнити всі ці результати та розробити необхідні заходи, які допоможуть їх усунути або зменшити вплив.

На практиці може трапитися, що встановлено високу ймовірність ризику (наприклад, при обробці особливої категорії даних) й ухвалено рішення, що всі необхідні заходи з безпеки даних уже реалізовані, потрібно лише їх контролювати. Однак варто провести додаткові консультації із зацікавленими сторонами, адже, враховуючи розвиток технологій, можуть з'явитися нові методи роботи з ризиками.

Усі результати роботи в цій сфері варто документувати. Це не означає, що треба створювати додаткові бюрократичні процедури, а навпаки — шукати нові механізми контролю.

Ризики виникають не тільки через внутрішні, а й зовнішні причини. Наприклад, недосконалість законодавства, відсутність відповідних механізмів регуляції тощо. У такому випадку можна звернутися до контролюючого органу за роз'ясненнями, як діяти в тій чи іншій ситуації. Якщо вони стосуються процесів обробки, що здійснюються на території України, — до Уповноваженого Верховної Ради України з прав людини, якщо інших країн, — тоді до відповідних локальних органів.

Що робити з цим далі?

Відповідь очевидна — треба інтегрувати результати оцінювання в діяльність установи та визначити подальші дії тих, хто буде відповідати за цей процес. Це один з найважливіших і часто найскладніших елементів усього циклу аналізу, бо від ефективності впровадження його результатів залежить відповідь на питання: чи все правильно зроблено?

Інколи результати оцінювання складно інтегрувати в поточну діяльність або ж з'являється сумнів, чи все було зроблено правильно. Тому цілком нормально повторити процес ще раз, перш ніж остаточно затверджувати подальший план дій.

Як оцінювати зміст аналізу ризиків?

Таке питання може виникнути, якщо оцінювання сприйнято не як формальність, а необхідний інструмент для забезпечення захисту персональних даних. Це означає, що в результатах повинні розглядатися не тільки виявлені ризики, а й усі документи, які пов'язані з цим процесом.

Наприклад, серед питань, які можна поставити:

- чи достатньою мірою ідентифіковані й мінімізовані ризики;
- чи такі дії дають змогу продовжити (або розпочати) обробку персональних даних;
- чи враховано дотримання загальних принципів захисту даних (про які згадано в першому розділі)?

Наприклад, у країнах ЄС, якщо були виявлені ризики та не реалізовані належні заходи з їх зниження, національний контролюючий орган (залежно від країни, де здійснюється обробка) може видати офіційне попередження для усунення ризиків. Зазвичай у попередженні будуть пояснені причини побоювань і вказані кроки, які варто зробити, щоб уникнути будь-яких порушень. Якщо виникнуть більш серйозні проблеми, то можуть накласти обмеження або заборону на обробку даних.

3.2. Учасники процесу аналізу ризиків

З погляду менеджменту добре, коли є відповідальна особа за обробку та захист персональних даних, у тому числі за проведення оцінювання ризиків. Звичайно, що цю роботу можна передати на аутсорсинг, але все одно відповідальність несе особа, що обробляє інформацію (або керівництво). З практичного погляду до аудиту варто залучити:

- відповідальну за обробку та захист даних особу, якщо така визначена;
- осіб, що відповідають за технічну безпеку систем;
- інших експертів, які дотичні до цієї сфери діяльності.

Якщо залучаються зовнішні спеціалісти, тоді варто з ними порадитися:

- Чи потрібно проводити оцінювання ризиків (або DPIA). Якщо так, тоді для яких саме операцій обробки даних?
- З огляду на діяльність організації цей процес краще робити власними силами чи віддати на аутсорсинг?
- Які заходи варто зробити для зниження ризиків?
- Чи правильно здійснювалося оцінювання раніше?
- Який очікуваний результат і як він буде інтегрований?

3.3. Публікація результатів оцінювання впливу на захист даних

Менеджмент з питань управління даними умовно складається з циклу таких робіт: планування — виконання — перевірка — дія.

Таким чином, його можна розглядати як засіб для сприяння дотриманню правил конфіденційності відповідно до національних і міжнародних стандартів. Результати проведення оцінювання ризиків повинні містити рекомендації щодо відповідних заходів, які демонструватимуть рівень забезпечення безпеки даних під час їх обробки (приклад звіту з оцінювання ризиків у додатках).

Публікація окремих результатів звіту буде демонструвати забезпечення принципу прозорості та підзвітності діяльності ОМС. Це

може допомогти зміцнити довіру суспільства до того, наскільки законною є робота у сфері захисту даних.

Наприклад, у країнах ЄС часто деякі організації створюють для себе більш суворі правила, ніж вимагає GDPR, щоб бути ще прозорішими у сфері обробки персональних даних.

І наостанок, публікація звіту може допомогти іншим суб'єктам узгодити свою діяльність із законом. Зверніть увагу, поширюючи свої знання і досвід, обов'язково зазначте, що процес оцінювання ризиків індивідуальний за структурою та змістом, бо інші суб'єкти, узявши ваш звіт за шаблон можуть не звернути увагу на важливі речі у своїй діяльності[44].

Як підійти до публікації результатів?

У разі публікації звіту варто подбати про комерційну таємницю, інтелектуальну власність і захист даних осіб, які можуть згадуватися у звіті. Прозорість діяльності — не означає розкриття «секретного рецепта» діяльності установи.

Публічний звіт може передбачати оприлюднення структури або шаблона, яким користується організація. Тому варто обміркувати всі переваги та ризики публікації звіту перш ніж ухвалювати таке рішення.

Не забудьте, будь ласка, про те, що оцінювання ризиків — це не одноразова робота, а систематичний процес!

44 Розкриття звіту DPIA не є обов'язковим відповідно до GDPR, хоча існує зобов'язання надати інформацію суб'єкту даних про обробку його (її) особистих даних (стаття 5 (1) (a) і статті 12-14 GDPR).

ВИСНОВКИ

Оцінювання ризиків — непростий процес, який потребує часу та чіткого розуміння всього циклу обробки персональних даних. Загалом його головна мета — відповісти на важливі питання:

- Які існують ризики?
- Які джерела їх виникнення?
- Які наслідки можуть настати?
- Як це відбувається?
- Що потрібно зробити, щоб їх усунути?

Бажано оцінювати ризики для кожної операції з обробки персональних даних, а особливо тієї, яка може становити високий рівень загрози для прав і свобод людини. Це особливо актуально у випадку впровадження нової технології, зміни цілей, роботи з інформацією вразливих груп населення тощо. У різних країнах світу, де діє закон про захист персональних даних, зазвичай рекомендують проводити систематичне оцінювання ризиків, бо це корисний інструмент, який допомагає уникнути порушень прав і свобод людини. Для цього варто залучити спеціалістів, які, використовуючи певні методології, комплексно проаналізують діяльність у сфері обробки та захисту персональних даних, визначать ключові ризики та підготують обґрунтовані рекомендації, як їх усунути або мінімізувати. Увесь цей процес потрібно документувати, щоб у разі виникнення спірних ситуацій можна було пояснити, чому були ухвалені ті чи інші рішення та що саме стало підставою для них.

Немає єдиного шаблона, методології чи інструкції, які підходили б усім. Оцінювання ризиків не робиться для формальних звітів або заради «галочки». Воно потрібно для того, щоб підібрати заходи для належного захисту персональних даних, завчасно зрозуміти можливі наслідки своїх дій.

Бути готовими до ідентифікації ризиків і мати можливості боротися з ними — саме такий підхід допомагає створити репутацію сильної та стабільної установи, якій можна довіряти та співпрацювати.

І наостанок, перелік контрольних дій, що потрібно зробити для організації процесу оцінювання ризиків у сфері обробки та захисту персональних даних:

- ухвалити політику, у якій буде визначено, коли потрібно проводити оцінювання ризиків (DPIA) (наприклад, у стратегії

діяльності ОМС, структурного підрозділу, установи або конкретного проєкту);

- розробити структуру та зміст методології, яка буде відповідати вимогам організації;
- підвищити обізнаність про ризики та методи аналізу серед персоналу;
- визначити відповідальних осіб і залучити компетентних осіб;
- переконатися, що ця процедура здійснюється ще до початку реалізації проєкту або систематично в певний проміжок часу;
- не забути проконсультуватися із зацікавленими сторонами щодо змісту та результатів;
- включити в процес оцінювання роботу з розпорядниками та третіми особами;
- переконатися, що інформація, що міститься в оцінюванні, відповідає вимогам законодавства і це детально описано у звіті;
- якщо результати оцінювання показують, що обробка даних може становити високий ризик і його неможливо зменшити, проконсультуватися з контролюючим органом у цій сфері;
- проаналізувати наявні процеси управління ризиками й переконатися в їх узгодженості та зв'язку з процесами оцінювання;
- переконатися, що вся необхідна документація легко доступна для використання співробітниками і що ви навчили їх того, як проводити оцінювання;
- проводити навчання, заохочувати особисту відповідальність;
- чітко викласти свій підхід до захисту даних і розподілити обов'язки керівництва;
- оцінювати й визначати сфери, які можуть викликати проблеми у сфері захисту даних або дотримання вимог безпеки, і вносити їх до реєстру ризиків.

ДЖЕРЕЛА

Guidelines on Data Protection Impact Assessment (DPIA) [Електронний ресурс] – Режим доступу до ресурсу: *https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236*

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: *https://www.kmu.gov.ua/storage/app/media/uploaded-files/es-2016679.pdf*

«The Practical Guide for Data Protection Impact Assessments subject to the GDPR» published by the AEPD.

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

Data protection impact assessments, ICO [Електронний ресурс] – Режим доступу до ресурсу: *https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/*

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [Електронний ресурс] – Режим доступу до ресурсу: *http://data.europa.eu/eli/dir/2002/58/oj*

EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (Version 2.0, Oct 2020) [Електронний ресурс] – Режим доступу до ресурсу: *https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201904_dataprotection_by_d esign_and_by_default_v2.0_en.pdf*

Center for Information Policy Leadership (CIPL), Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR (Dec 2016) [Електронний ресурс] – Режим доступу до ресурсу: *https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf*

ДОДАТОК 1

Контрольний список питань для самоперевірки

- ☑ Є опис характеру, обсягу, контексту й мети обробки даних.
- ☑ Усі процеси задокументовані, зокрема укладені договірні відносини з розпорядниками.
- ☑ Є практика проведення консультацій з окремими особами (або їх представниками) й іншими відповідними зацікавленими сторонами.
- ☑ Є комунікація з Уповноваженим Верховної Ради України з прав людини[45] з питань обробки даних.
- ☑ Є практика перевірки того, чи обробка даних необхідна і співмірна цілям.
- ☑ Є опис (інструкція, положення, політика) того, як забезпечується дотримання принципів захисту даних.
- ☑ Здійснюється об'єктивне оцінювання ймовірності будь-яких ризиків для прав і інтересів людей.
- ☑ Є сплановані заходи, які можуть бути вжиті для усунення або зниження високих ризиків.
- ☑ Усі результати та ухвалені рішення в межах аналізу (оцінювання) фіксуються, включаючи будь-які розбіжності в думках з особами, з якими проводилися консультації.
- ☑ Забезпечено можливість інтегрувати заходи, визначені за результатами оцінювання та необхідні для зменшення або усунення ризиків.
- ☑ Є практика перегляду попередніх оцінювань і їх аналізу.
- ☑ Визначено, коли необхідно проводити оцінювання, і список документів (законодавства), відповідно до якого воно проводиться.

---

45 Контролюючий орган у сфері захисту персональних даних.

- ☑ Сформовані очікування щодо результатів оцінювання: методологія, процес проведення та фінальний звіт.
- ☑ Під час оцінювання враховані всі аспекти взаємодії з розпорядниками інформації під час передачі даних.
- ☑ Під час оцінювання враховані всі положення законодавства про забезпечення прав суб'єктів даних.
- ☑ У звіті про оцінювання ризиків передбачений аналіз того, як організація дотримується всіх принципів обробки та захисту даних (законності, прозорості, мінімізації даних тощо)[46].
- ☑ Усі заходи зі зниження або усунення ризиків детально описані та запропоновані рішення.
- ☑ З приводу заходів, щодо яких існують сумніви, проведені додаткові консультації.
- ☑ Є графік наступних процедур аудиту, а також виконання рекомендацій і завдань, визначених у межах попереднього оцінювання.

46 Див. розділ 1 цього посібника.

ДОДАТОК 2

Приклади результатів загального звіту про оцінювання впливу[47]

Немає єдиного шаблона та структури методології оцінювання ризиків. Усе залежить від багатьох факторів, що напряму стосуються конкретної установи. Але є базові елементи, з яких може складатися звіт. Наведемо приклад структури такого звіту.

№	ЗМІСТ	ОПИС
1.	Зміст	Структура та зміст звіту про оцінювання ризиків.
2.	Коротке резюме	Про ОМС (або його структурний підрозділ, підпорядковану установу, де здійснюється оцінювання ризиків у сфері захисту даних), його діяльність, правові підстави, команду, локацію, можливо, причини, які стали передумовою для проведення оцінювання ризиків.
3.	Предмет оцінювання	Конкретна сфера аналізу (сервіси, послуги, вид діяльності, технології тощо).
4.	Мета	Які процеси обробки персональних даних підлягають оцінюванню (наприклад, збір, передача, використання, зберігання або видалення даних або весь цикл обробки даних).
5.	Підстава для проведення	Поточне оцінювання відповідно до вимог закону або ініційоване контролюючим органом, урядом, за рішенням суду тощо.
6.	Ключові завдання	Перелік завдань у межах аудиту (оцінювання ризиків).

47 Наведені приклади не є шаблоном, а швидше можливим сценарієм оцінювання.

7.	Вимоги законодавства	Перелік норм законів, стандартів, міжнародних правил, внутрішніх документів тощо.
8.	Особливі вимоги	Урядові, рекомендації контролюючих органів у цій сфері або рішення суду тощо. Наприклад, трапився інцидент з безпекою даних, який призвів до необхідності аналізу певних процедур з обробки даних.
9.	Короткий зміст висновків попереднього звіту	Якщо раніше вже проводилося оцінювання ризиків. Короткі тези висновків і рекомендацій.
10.	Вид і категорія даних, які обробляються	Перелік даних, які збирає організація.
11.	Особливі категорії даних	Перелік та опис даних, які становлять особливий ризик.
12.	Процеси обробки, які підлягають оцінюванню впливу	Перелік та опис процесів обробки персональних даних, зокрема тих, що становлять особливий ризик. Оцінювання цих процесів з погляду ризику та категоризація за рівнем загроз.
13.	Законна підстава та цілі обробки	Перелік підстав для кожного виду обробки та цілей. Співвідношення пропорційності та сумісності цілей.
14.	Дотримання принципів обробки даних	Аналіз дотримання принципів обробки даних: пропорційності, обмеження мети, законності тощо.
15.	Джерела збору даних	Усі джерела, через які збирається інформація (онлайн та офлайн).

16.	Локалізація	Де здійснюється збір і подальша обробка даних (країна, місто).
17.	Технічний аналіз і моделювання сценаріїв	Аналіз технічного захисту систем.
18.	Категорії суб'єктів персональних даних	Категорії суб'єктів і можливі для них загрози (наприклад, за такими ознаками: вік, соціальний статус, стать, уподобання або переконання тощо).
19.	Окремі застереження	Попередні скарги, звернення тощо від суб'єктів персональних даних.
20.	Доступ до даних третіх осіб	Опис підстав, мети та умов передачі персональних даних третім особам, а також їх перелік. Окрім того, у звітах може вказуватися, хто найчастіше запитує інформацію та з якої причини. Наприклад, може виявитися, що до установи (конкретного структурного підрозділу) часто надходять адвокатські запити чи запити від органів правопорядку про надання доступу до певних видів і категорій даних. Це може бути сигналом для наявних або потенційних ризиків.
21.	Розпорядники інформації	Перелік розпорядників, мета, підстави та умови передачі даних. Наприклад, деталі про договірні відносини з розпорядниками персональних даних: цілі роботи, відповідно до яких отримана згода на обробку даних; перелік дій (операцій) з даними, які здійснюються розпорядником у межах договору; обов'язки щодо конфіденційності інформації.
22.	Транскордонна передача даних	Країна, умови та підстави для транскордонної передачі.

23.	Зберігання даних	Як, де та який час зберігається інформація. Умови та процедури видалення.
24.	Матриця оцінювання ризиків	Визначення рівня впливу, ймовірності виникнення шкоди (матриця оцінювання ризиків) для кожного окремого процесу.
25.	Висновки організації за результатами	Результати оцінювання ризиків.
26.	Висновки та рекомендації, надані зацікавленими сторонами	Перелік сторін і короткий опис висновків і рекомендацій.
27.	Суперечливі висновки та окремі застереження	Короткий аналіз (опис) висновків, які були надані особами, що проводили аудит (спільні інтереси, суперечливі позиції, застереження пропозиції).
28.	Детальний опис заходів зі зменшення або усунення ризиків	Рекомендації щодо реагування на кожний окремий процес / ризик.
29.	Окремі рекомендації	Окремі рекомендації щодо стратегії роботи з даними або процедур оцінювання ризиків на майбутнє.

ДОДАТОК 3

***Стаття 35 Загального регламенту захисту даних «Оцінювання впливу на захист даних»** (Article 35 GDPR «Data protection impact assessment»)*[48]

1. Якщо тип опрацювання, зокрема з використанням нових технологій, і зважаючи на специфіку, обсяг, контекст і цілі опрацювання, ймовірно призведе до виникнення високого ризику для прав і свобод фізичних осіб, контролер, до здійснення опрацювання, повинен провести оцінювання впливу передбачених операцій опрацювання на захист персональних даних. Єдине оцінювання може стосуватися низки подібних операцій опрацювання, що становлять подібні високі ризики.

2. Контролер повинен звернутися за рекомендаціями до співробітника з питань захисту даних, якщо його призначено, у ході проведення оцінювання впливу на захист даних.

3. Оцінювання впливу на захист даних, вказане в параграфі 1, є необхідним, зокрема, у випадку:

(a) систематичного та масштабного оцінювання персональних аспектів, що стосуються фізичних осіб, яке ґрунтується на автоматизованому опрацюванні, в тому числі, профайлінгу, та на якому ґрунтуються рішення, що мають юридичні наслідки щодо фізичної особи чи подібним чином істотно впливають на фізичну особу;

(b) широкомасштабного опрацювання спеціальних категорій даних, вказаних у статті 9(1), та персональних даних про судимості і кримінальні злочини, вказані в статті 10; або

(c) систематичного та широкомасштабного моніторингу зони, що знаходиться у відкритому доступі.

---

48 Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року «Про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних): *https://www.kmu.gov.ua/storage/app/media/uploaded-files/es-2016679.pdf*

4. Наглядовий орган повинен розробити і оприлюднити перелік операцій опрацювання, на які поширюється вимога проведення оцінювання впливу на захист даних відповідно до параграфа 1. Наглядовий орган повідомляє Раду про такі переліки, як вказано в статті 68.

5. Наглядовий орган може також розробляти і оприлюднювати перелік операцій опрацювання, на які не поширюється вимога проведення оцінювання впливу на захист даних. Наглядовий орган повинен повідомляти Раду про такі переліки.

6. До ухвалення переліків, вказаних у параграфах 4 і 5, компетентний наглядовий орган повинен застосовувати механізм послідовності, вказаний у статті 63, якщо такі переліки включають опрацювання даних, пов'язане з пропонуванням товарів або послуг суб'єктам даних або моніторингом їхньої поведінки в декількох державах-членах, або можуть істотно впливати на вільний рух персональних даних у межах Союзу.

7. Оцінювання повинне містити принаймні:

(a) систематичний опис передбачених операцій опрацювання та цілі опрацювання, в тому числі, за необхідності, законний інтерес контролера;

(b) оцінювання необхідності та пропорційності операцій опрацювання щодо цілей;

(c) оцінювання ризиків для прав і свобод суб'єктів даних, вказаних у параграфі 1; та

(d) заходи, передбачені для боротьби з ризиками, в тому числі, гарантії, заходи безпеки та механізми забезпечення захисту персональних даних та доведення відповідності цьому Регламенту, з урахуванням прав і законних інтересів суб'єктів даних та інших залучених осіб.

8. Необхідно належним чином враховувати дотримання відповідними контролерами або операторами затверджених кодексів поведінки, вказаних у статті 40, під час оцінювання впливу операцій опрацювання, які здійснюють такі контролери або оператори, зокрема, для цілей оцінювання впливу на захист даних.

9. У разі необхідності, контролер повинен ознайомитися з думками суб'єктів даних або їхніх представників щодо запланованого опрацювання, без обмеження захисту комерційних або суспільних інтересів або безпеки операцій опрацювання.

10. Якщо опрацювання відповідно пункту (c) або (e) статті 6(1) має законодавчу базу відповідно до законодавства Союзу або законодавства держави-члена, яке поширюється на контролера, таке законодавство регулює конкретну операцію опрацювання чи відповідну низку операцій, і якщо оцінювання впливу на захист даних вже було проведено як частину загального оцінювання впливу в контексті ухвалення такої законодавчої бази, параграфи 1—7 не застосовують, за винятком, якщо держави-члени вважають за необхідне провести таке оцінювання до здійснення опрацювання даних.

11. У разі необхідності, контролер повинен провести перевірку, щоб пересвідчитися, чи здійснюють опрацювання з урахуванням оцінювання впливу на захист даних, принаймні — у разі зміни ризику, який становлять операції опрацювання.

Стаття 36 «Попередня консультація»

1. Контролер повинен надати консультацію наглядовому органу до початку здійснення опрацювання, якщо оцінка впливу на захист даних за статтею 35 свідчить про те, що опрацювання призведе до виникнення високого ризику в разі відсутності заходів, які вживає контролер для зниження ризику.

2. Якщо наглядовий орган вважає, що заплановане опрацювання, вказане в параграфі 1, може порушити цей Регламент, зокрема, якщо контролер недостатньо ідентифікував або знизив ризик, наглядовий орган, протягом періоду до восьми тижнів після отримання запиту на консультацію, повинен надати контролеру письмові рекомендації та, в разі необхідності, оператору, а також може використовувати будь-які свої повноваження, вказані в статті 58. Цей період може бути подовжено на шість тижнів, з огляду складність запланованого опрацювання. Наглядовий орган інформує контролера та, в разі необхідності оператора, про будь-яке таке подовження протягом одного місяця з дати отримання запиту на

консультацію разом з інформацією про причини такої затримки. Такі періоди може бути призупинено до отримання наглядовим органом інформації, яку він запитував для цілей консультації.

3. Надаючи консультацію наглядовому органу відповідно до параграфа 1, контролер повинен надати наглядовому органу:

(a) в разі необхідності, інформацію про відповідні обов'язки контролера, об'єднаних контролерів і операторів, залучених до опрацювання, зокрема, для опрацювання в межах групи підприємств;

(b) цілі та засоби запланованого опрацювання;

(c) засоби та гарантії, передбачені для захисту прав і свобод суб'єктів даних відповідно до цього Регламенту;

(d) в разі необхідності, контактні дані співробітника з питань захисту даних;

(e) оцінку впливу на захист даних, передбачену в статті 35; і

(f) будь-яку іншу інформацію, яку запитує наглядовий орган.

4. Держави-члени повинні надати наглядовому органу консультацію під час підготування пропозиції для законодавчого інструменту, який повинен ухвалити національний парламент, або регуляторного інструменту на підставі такого законодавчого інструменту, що стосується опрацювання.

5. Без обмеження положень параграфа 1, законодавство держав-членів може вимагати від контролерів проводити консультації та отримувати попередній дозвіл від наглядового органу щодо опрацювання контролером для реалізації завдання, яке виконує контролер для цілей суспільного інтересу, в тому числі, опрацювання в сфері соціального захисту і охорони суспільного здоров'я.

Стандарт ISO/IEC 27701

(EN) ISO/IEC 27701, adopted in 2019, added additional ISO/IEC 27002 guidance for PII controllers.

Here is the relevant paragraph to article 35 GDPR:

7.2.5 Privacy impact assessment

Control

The organization should assess the need for, and implement where appropriate, a privacy impact assessment whenever new processing of PII or changes to existing processing of PII is planned.

Implementation guidance

PII processing generates risks for PII principals. These risks should be assessed through a privacy impact assessment. Some jurisdictions define cases for which a privacy impact assessment is mandated. Criteria can include automated decision making which produces legal effects on PII principals, large scale processing of special categories of PII (e. g. health-related information, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data or biometric data), or systematic monitoring of a publicly accessible area on a large scale.

The organization should determine the elements that are necessary for the completion of a privacy impact assessment. These can include a list of the types of PII processed, where the PII is stored and where it can be transferred. Data flow diagrams and data maps can also be helpful in this context (see 7.2.8 for details of records of the processing of PII that can inform a privacy impact or other risk assessment).

Other information

Guidance on privacy impact assessments related to the processing of PII can be found in ISO/IEC 29134.