Омбудсман України
Ombudsman of Ukraine

MOVING FORWARD TOGETHER

EU4DigitalUA

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В ДІЯЛЬНОСТІ СУБ'ЄКТІВ ВЛАДНИХ ПОВНОВАЖЕНЬ

РОЗ'ЯСНЕННЯ

Авторка
Уляна Шадська
експертка проєкту EU4DigitalUA

Дизайн та верстка
Аліна Пірлік
експертка проєкту EU4DigitalUA

ПЕРЕДМОВА

Останні декілька років в Україні здійснюється процес цифрової трансформації в системі державного управління. Більшість адміністративних послуг автоматизовано та переведено в онлайн режим. Нові технологічні рішення передбачають обробку та аналіз великого масиву інформації, яка містить персональні дані. Безперечно, розвиток інновацій має великий спектр переваг, але поряд з цим, з'являються ризики для прав і свобод людини, зокрема, що пов'язані з несанкціонованими витоками її особистих даних.

Забезпечення недоторканності приватного й сімейного життя людини, передбачене статтею 32 Конституції України, — є одним із пріоритетних напрямків розвитку держави та її демократичних принципів. У 2011 році було прийнято Закон України «Про захист персональних даних», коли ще не поширювалася цифровізація державних та приватних сервісів. Національне законодавство повинно відповідати змінам, які відбуваються в цій області.

Тому у 2014 році Україна, підписавши Угоду[1] про асоціацію з ЄС, серед іншого, взяла на себе зобов'язання щодо забезпечення захисту персональних даних відповідно до європейських стандартів. Це стало обґрунтованою підставою, щоб усі суб'єкти владних повноважень розпочали діяти за єдиними міжнародними правилами. Органи державної влади та місцеве самоврядування[2] повинні самостійно впроваджувати організаційні та технічні заходи щодо захисту персональних даних, в залежності від специфіки своєї діяльності.

У зв'язку з цим, експерти проєкту EU4DigitalUA у взаємодії з представниками Офісу Омбудсмана розробили роз'яснення щодо необхідних кроків для організації роботи з персональними даними, зокрема в державних органах влади. Документ складається із трьох розділів: перший присвячений теоретичним засадам, а інші два — надають відповіді на практичні питання щодо процесів обробки й захисту конфіденційної інформації. Варто зауважити, що запропоновані тези детально не розкривають зміст положень закону, а допомагають розібратися в його суті.

1 Угода про асоціацію між Україною та Європейським Союзом, Європейським співтовариством з атомної енергії та їх державами-членами, з іншого боку (Угоду ратифіковано із заявою Законом № 1678-VII від 16.09.2014 року), де у статті 15 «Захист персональних даних» визначено, що: «Сторони домовилися співпрацювати з метою забезпечення належного рівня захисту персональних даних відповідно до найвищих європейських і міжнародних стандартів, зокрема відповідних документів Ради Європи».
2 Надалі у тексті також буде використовуватися термін «установа».

ЗМІСТ

РОЗДІЛ 1

ЗАГАЛЬНІ ПОЛОЖЕННЯ

Органи державної влади для виконання своїх функцій обробляють великий обсяг різної інформації, значна частина якої містить персональні дані. Це означає, що вони повинні дотримуватися положень національного законодавства та міжнародних положень, що регулюють процес їх обробки та захисту.

У першому розділі запропоновані роз'яснення щодо змісту основних термінів й правил, які там визначені. Адже правильне розуміння основних понять має значення та допомагає зрозуміти, чи буде законною діяльність в даній сфері.

ЩО ОЗНАЧАЄ ПРАВО НА ПРИВАТНЕ ТА СІМЕЙНЕ ЖИТТЯ?

Термін «приватність» використовується у повсякденному житті, політичних та юридичних дискусіях. Понад століття тому суспільство заговорило про приватність із тієї ж причини, яка робить цю тему актуальною й сьогодні, — через розвиток технологій та ризики через втручання в особисте життя людини, зокрема з боку держави.

У 1948 році право на приватність було зафіксовано у статті 12 Загальної декларації прав людини, а в 1950-му році — у статті 8 Європейської конвенції з прав людини і основоположних свобод. Попри те, що становлення цього права відбулось вже давно, але по сьогодні актуальні залишаються питання: що таке приватне та сімейне життя?

Сімейне життя — це особисті майнові та немайнові відносини між подружжям, іншими членами сім'ї, які здійснюється на засадах, визначених у Сімейному кодексі України. Особистим життям фізичної особи є її поведінка у сфері особистісних, сімейних, побутових, інтимних, професійних та інших стосунків поза межами суспільної діяльності, яка здійснюється, зокрема, під час виконання особою функцій держави або органах місцевого самоврядування.

У рішенні[3] від 20 січня 2012 року No2-рп/2012 Конституційний Суд України зазначив, що неможливо визначити абсолютно всі види поведінки фізичної особи у сферах особистого та сімейного життя, оскільки вони не вичерпні й реалізуються в різноманітних відносинах майнового та немайнового характеру, стосунках, явищах, подіях тощо. Право на приватне та сімейне життя є засадничою цінністю, необхідною для повного розквіту людини в демократичному

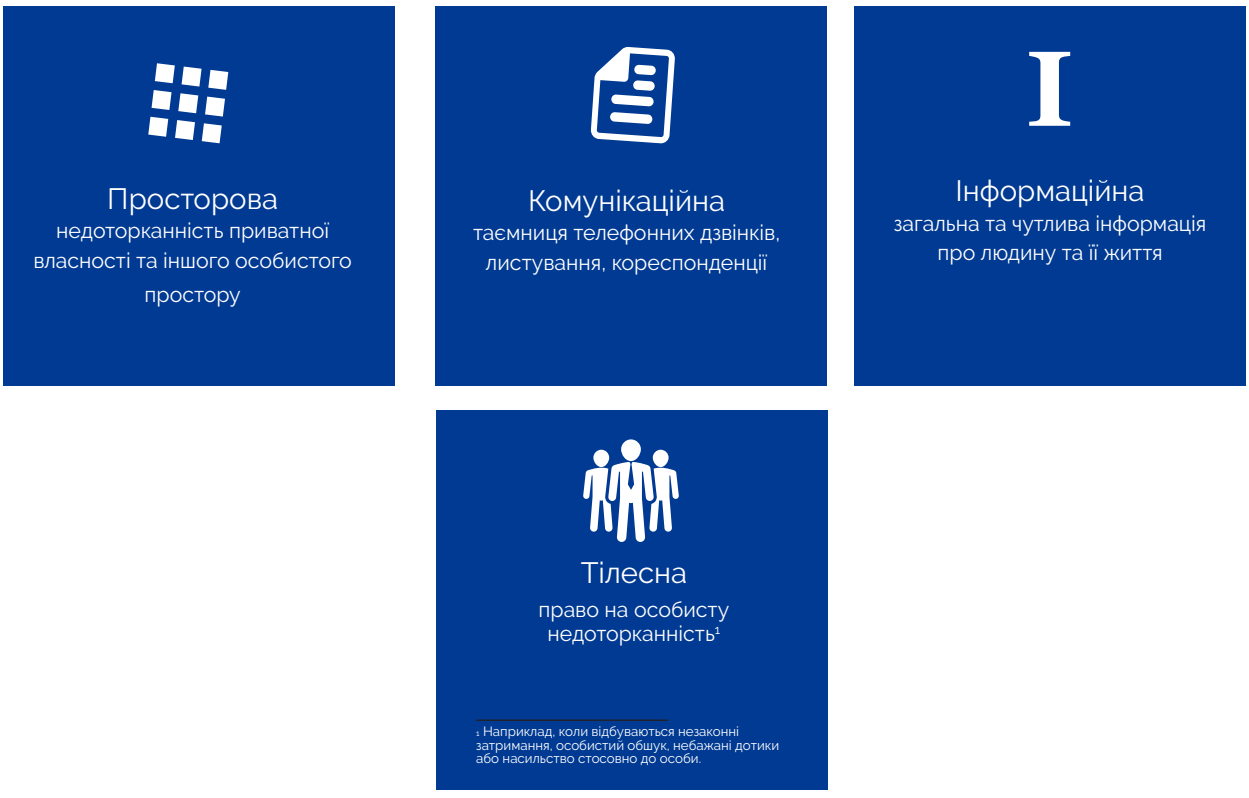
3 Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України. Режим доступу: http://zakon2.rada.gov.ua/laws/show/v002p710-12

суспільстві, та розглядається як право на автономне буття незалежно від держави, юридичних й фізичних осіб.

Європейський суд з прав людини (надалі — ЄСПЛ) також узагальнив практику щодо тлумачення поняття «приватне життя» й вказав, що неможливо дати йому вичерпне визначення, бо воно охоплює фізичну та психологічну недоторканість особи та може стосуватися різних аспектів її соціальної самоідентифікації. (Рішення ЄСПЛ «S. та Марпер проти Сполученого Королівства», від 04 грудня 2008 року, No30562/04 та 30566/04)[4].

У цьому контексті важливо зазначити, що у різних матеріалах та публікаціях на тему захисту персональних даних, органи державної влади часто використовують термін «право на приватність», але це не завжди коректно, бо приватність та персональні дані це не одне й теж. Передусім, приватність ідентична виразу «приватне життя», і, як зазначено вище, тут мова йде не тільки про особисті дані людини. У теоретичних засадах визначають декілька видів приватності:

4 Посібник з європейського права у сфері захисту персональних даних. Режим доступу: https://rm.coe.int/168059b6a8.



КОЛИ ДАНІ ПРО ОСОБУ, ЯКА ОБІЙМАЄ ПОСАДУ, ПОВ'ЯЗАНУ ЗІ ЗДІЙСНЕННЯМ ФУНКЦІЙ ДЕРЖАВИ, НАЛЕЖАТЬ ДО КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ?

Питання щодо конфіденційності інформації про особу, яка обіймає державну посаду та членів її сім'ї, було розглянуто Конституційним Судом України. У рішенні Суду зазначено[5], що належність інформації про фізичну особу до конфіденційної визначається в кожному конкретному випадку. Перебування особи на державній посаді передбачає не тільки гарантії захисту прав цієї особи, а й додаткові правові обтяження. Публічний характер, як самих органів — суб'єктів владних повноважень, так і їх посадових осіб, вимагає оприлюднення певної інформації для формування громадської думки про довіру до влади та підтримки її авторитету у суспільстві.

Парламентська Асамблея Ради Європи у своїй Резолюції від 25 грудня 2008 року № 1165 (1998) вказала, що публічні особи повинні усвідомлювати, що особливий статус, який вони мають у суспільстві, автоматично збільшує рівень тиску на приватність їхнього життя (пункт 6). Згідно із законодавством України не належать до інформації з обмеженим доступом, зокрема: декларації про доходи осіб та членів їхніх сімей, які претендують на зайняття чи займають виборну посаду в органах влади або обіймають посаду державного службовця, службовця органу місцевого самоврядування першої або другої категорії ; персональні дані фізичної особи, яка претендує зайняти чи займає виборну посаду (у представницьких органах) або посаду державного службовця першої категорії[6], за винятком інформації, яка відповідно до закону визначена такою, що належить до інформації з обмеженим доступом[7]; відомості про незаконні дії органів державної влади, органів місцевого самоврядування, їх посадових та службових осіб[8].

Разом з тим, аналізуючи питання щодо поширення інформації про сімейне життя такої особи, Конституційний Суд України враховує, що персональні дані можуть ще стосуватися не лише цієї особи, а й членів її сім'ї, яким Конституція України гарантує право на невтручання в їхнє особисте і сімейне життя, крім випадків, визначених законом. Тому, тут немає однозначної відповіді, бо у кожному окремому випадку необхідно знаходити баланс та вирішувати, коли поширення персональних даних про таких фізичних осіб та членів сім'ї може мати суспільний інтерес та є необхідним.

5 Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України. Режим доступу: http://zakon2.rada.gov.ua/laws/show/v002p710-12

6 Стаття 6 Закону України «Про доступ до публічної інформації».
7 Стаття 5 Закону України «Про захист персональних даних».
8 Стаття 21 Закону України «Про інформацію».

ЩО ТАКЕ ПЕРСОНАЛЬНІ ДАНІ?

Персональні дані — відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. А саме — мова йде про будь-яку інформацію, яка відображає фізичну, соціальну, культурну або іншу ідентичність людини. Персональні дані можуть бути виражені у різних формах, наприклад: фото, відео (зображення особи); цифр (наприклад, ідентифікаційний код, номер телефону); звуку (наприклад, голос) тощо.

У кожному окремому випадку потрібно аналізувати зміст інформації та відповідати на питання, чи дозволить сукупність цих даних прямо, чи опосередковано ідентифікувати фізичну особу?

Наприклад, називати ім'я людини — найпоширеніший спосіб ідентифікації когось, але у світі може бути багато людей з однаковим ім'ям. Додаткові відомості (певні ознаки) й будуть вважатися ідентифікаторами, які нададуть можливість відрізнити одну людину від іншої.

Чому важливо з цим розібратися?

У процесі обробки персональних даних ведеться окремий реєстр (детальніше про це далі у тексті), у якому зазначається уся характеристика інформації, що збирається. Тобто, коли посадова особа не знає, яка інформація належить до персональних даних, може не занести її до реєстру та, відповідно, не виконувати необхідні процедури щодо їх захисту. Це все може призвести до порушення закону.

Чи є номер телефону персональними даними?

Це питання є досить поширене серед державних службовців і не тільки. Як вже було зазначено, до персональних даних відноситься будь-яка інформація, яка може прямо або опосередковано ідентифікувати фізичну особу. Тобто, коли дані однозначно вказують на конкретного суб'єкта, або частково (опосередкована ідентифікація) — коли потрібні ще додаткові відомості. Це означає, що попри те, що сам по собі номер телефону може нічого не говорить про особу його власника, але поєднання з додатковими відомостями допомагає не тільки ідентифікувати людину, а й отримати багато іншої інформації про її приватне та сімейне життя. Отже, номер телефону, державний номерний знак автомобіля або інша інформація у формі цифр, належить до персональних даних, зокрема категорії метаданих (даних про дані).

ЯКІ Є ВИДИ ТА КАТЕГОРІЇ ПЕРСОНАЛЬНИХ ДАНИХ?

Закон розділяє персональні дані на дві категорії: загальні та особливі (або їх ще називають чутливі). Це необхідно для того, щоб визначити ступінь ризику, внаслідок їх незаконної обробки (наприклад, збирання чи несанкціонованого витоку).

Наприклад, до загальної категорії можна віднести прізвище та ім'я особи, інформація про її місце проживання, дані, записані в посвідченні водія; підпис; IP-адреси та ін. Тобто це будь-які відомості, які дозволять прямо або опосередковано ідентифікувати людини.

Особлива категорія має вичерпний перелік видів персональних даних. Це інформація про расове або етнічне походження; політичні, релігійні, світоглядні переконання; членство в політичних партіях та професійних спілках; засудження до кримінального покарання, а також даних, що стосуються здоров'я, статевого життя, біометричних або генетичних даних[9]. Тобто, це та інформація, яка може мати високий ризик для прав і свобод людини й потребує особливих умов для її обробки та захисту.

Крім того, наказом[10] Уповноваженого Верховної Ради України з прав людини передбачено додаткові категорії персональних даних, обробка яких становить особливий ризик для прав і свобод суб'єктів:

- притягнення до адміністративної відповідальності;
- застосування щодо особи заходів в рамках досудового розслідування;
- вжиття щодо особи заходів, передбачених Законом України «Про оперативно-розшукову діяльність»;
- вчинення щодо особи тих чи інших видів насильства;
- місцеперебування та/або шляхи пересування особи.

Тому, працюючи з персональними даними, необхідно розрізняти їх категорію, мати законні підстави для їх обробки, вести записи та здійснювати документування усіх дій з такою інформацією.

9 Стаття 7 Закону України «Про захист персональних даних».
10 Наказ Уповноваженого Верховної Ради України з прав людини від 08.01.2014 № 1/02-14 .

ЩО ТАКЕ ОБРОБКА ПЕРСОНАЛЬНИХ ДАНИХ?

Обробка персональних даних — це будь-яка з ними дія: збирання, реєстрація, накопичення, зберігання, використання, поширення, передача, знеособлення, видалення[11].

Слід взяти до уваги, що не можливо навести повний (виключний) перелік дій, що становлять обробку персональних даних, оскільки їх важко передбачити, особливо з огляду на розвиток технологій та появу нових видів і способів обробки. Щодо кожного етапу обробки персональних даних (наприклад, збору або передачі) має застосовуватися відповідна процедура регулювання.

ДЛЯ ЯКИХ ЦІЛЕЙ МОЖНА ОБРОБЛЯТИ ПЕРСОНАЛЬНІ ДАНІ?

Відповідно до статті 6 Закону України «Про захист персональних даних» мета обробки персональних даних має бути визначена в законах або інших нормативно-правових актах, положеннях, установчих документах, які регулюють діяльність конкретної установи. Тобто, згідно з загальним принципом «обмеження мети», необхідно заздалегідь обґрунтувати цілі збору персональних даних, адже надалі це стане запобіжником від їх незаконного використання.

11 Перелік дій, що передбачає процес обробки персональних даних, визначений у статті 2 Закону України «Про захист персональних даних».

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

- Чи визначено підстави, мету та завдання обробки персональних даних до початку їх обробки?
- Чи визначена мета в законах або інших нормативно-правових актах, що регулюють діяльність установи?
- Чи задокументовані ці цілі?
- Збір інформації здійснюються виключно в межах визначеної мети?

ЯКІ ПРАВОВІ ПІДСТАВИ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ?

Підставами[12] для обробки персональних даних для державних органів є:

1. Дозвіл на обробку персональних даних, наданий володільцю персональних даних відповідно до закону виключно для здійснення його повноважень.
2. Укладення та виконання правочину, стороною якого є суб'єкт персональних даних або який укладено на користь суб'єкта персональних даних чи для здійснення заходів, що передують укладенню правочину на вимогу суб'єкта персональних даних.
3. Захист життєво важливих інтересів суб'єкта персональних даних.
4. Необхідність виконання обов'язку володільця персональних даних, який передбачений законом.
5. Необхідність захисту законних інтересів володільця персональних даних або третьої особи, якій передаються персональні дані, крім випадків, коли потреби захисту основоположних прав і свобод суб'єкта персональних даних у зв'язку з обробкою його даних переважають такі інтереси.

У статті 19 Конституції України зазначається, що 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 органи влади (їх посадові особи) можуть здійснювати обробку персональних даних (будь-яку дію або сукупність дій) лише за наявності наданих повноважень, законної підстави й обґрунтованої мети та у спосіб, передбачений законом.

Тобто, не потрібно отримувати згоду суб'єкта персональних даних у тих випадках, коли збір такої інформації прямо передбачено законом та необхідний для виконання службового обов'язку чи реалізації повноважень. Разом з тим, недостатньо мати тільки повноваження, має бути ще обґрунтована мета та процедура, визначена у внутрішньо-розпорядчій документації.

Також важливо зазначити, що в межах діяльності органу державної влади кожна окрема її посадова особа також повинна мати окремо визначені повноваження щодо обробки персональних даних. Тобто, само по собі перебування на службі не дає ще права на роботу з такою інформацією, тільки в межах, визначених посадовою інструкцією або іншим внутрішньовідомчим актом.

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

ЯКИЙ ОБСЯГ ПЕРСОНАЛЬНИХ ДАНИХ МОЖНА ЗБИРАТИ?

Перед тим, як розпочинати обробку персональних даних, необхідно заздалегідь обґрунтувати цілі збору інформації. Відповідно до статті 6 Закону України «Про захист персональних даних» мета обробки персональних даних має бути визначена в законах або інших нормативно-правових актах, положеннях, установчих документах, які регулюють діяльність конкретної установи. На практиці установа може збирати дані для різних цілей. Тому, важливо, щоб такі дії були задокументовані у внутрішньо-відомчій документації.

ЩО ТАКЕ НАКОПИЧЕННЯ ПЕРСОНАЛЬНИХ ДАНИХ ТА ЯКИЙ ТЕРМІН ЇХ ЗБЕРІГАННЯ?

Накопичення та зберігання персональних даних є складовою їх обробки. Хоча ці поняття схожі за своєю суттю, проте є окремими видами обробки інформації.

Накопичення персональних даних передбачає дії щодо поєднання та систематизації відомостей про фізичну особу або внесення їх до відповідних баз. Зберігання ж персональних даних — це дії щодо забезпечення їх цілісності до відповідного режиму доступу[13]. Персональні дані повинні зберігатися не довше, ніж це необхідно для досягнення мети, якщо інше не передбачено законом[14]. Далі — персональні дані знищуються або передаються в архів. В окремих випадках строк зберігання може бути подовжено, але це має бути обґрунтовано та визначено у відповідних внутрішньо-розпорядчих документах.

13 Стаття 13 Закону «Про захист персональних даних».
14 Наказом Міністерства юстиції України № 578/5 від 12.04.2012 затверджений Перелік типових документів, що створюються під час діяльності державних органів, інших установ, підприємств та організацій, із зазначенням строків зберігання документів.

ЯКИЙ ПОРЯДОК ВИДАЛЕННЯ ПЕРСОНАЛЬНИХ ДАНИХ?

Видалення персональних даних — це дії, в результаті яких стає неможливим відновити їх зміст в інформаційних ресурсах або інших носіях, де вони зберігаються. Це важливо, адже на практиці зустрічаються випадки, коли видаляється інформація тільки з одного ресурсу, а при цьому залишається на інших.

Персональні дані підлягають видаленню або знищенню у разі:

1. закінчення строку зберігання персональних даних, визначеного згодою суб'єкта персональних даних на обробку цих даних або законом;
2. припинення правовідносин між суб'єктом персональних даних та володільцем чи розпорядником, якщо інше не передбачено законом;
3. видання відповідного припису Уповноваженого Верховної Ради України з прав людини або визначених ним посадових осіб Секретаріату Уповноваженого Верховної Ради України з прав людини;
4. набрання законної сили рішення суду щодо видалення або знищення персональних даних.

Також персональні дані видаляються або знищуються, якщо вони зібрані:

з порушенням вимог Закону України «Про захист персональних даних»;

Персональні дані, зібрані під час виконання завдань оперативно-розшукової чи контррозвідувальної діяльності, боротьби з тероризмом, видаляються або знищуються відповідно до вимог закону[15].

Необхідно скласти відповідний Акт (інший документ) про знищення персональних даних, у якому має бути зазначено:

- ◊ відомості про володільця персональних даних;
- ◊ перелік даних, які були знищені;
- ◊ прізвище, ім'я, по батькові, посаду осіб, які здійснили знищення персональних даних;
- ◊ перелік носіїв, де зберігалися дані (наприклад, найменування інформаційної системи, у разі автоматизованої обробки інформації);
- ◊ спосіб, причину, правові підстави та дату знищення персональних даних.

У випадку видалення персональних даних видалення має бути здійснено у такий спосіб, щоб унеможливити їх відновлення.

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

РОЗДІЛ 2

ОРГАНІЗАЦІЙНІ ЗАХОДИ ДЛЯ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

Органи державної влади самостійно визначають процедури для обробки та заходи безпеки персональних даних. Більшість порушень закону у даній сфері, пов'язані саме з організаційними процесами обробки інформації та відсутністю належного внутрішнього контролю.

Наприклад, може збиратися надлишковий обсяг персональних даних; здійснюватися їх обробка в цілях, несумісних з тими, з якими були зібрані спочатку; відсутні необхідні документи, які мають регулювати процедури обробки персональних даних; не призначена відповідальна особа там, де обов'язково це потрібно зробити згідно із законом тощо.

Для забезпечення належного рівня захисту персональних даних необхідно прийняти ряд заходів, які спочатку приведуть до поліпшення загальної ситуації, а в довгостроковій перспективі сприятимуть у становленні суспільства, де право на повагу до приватного життя буде гарантовано.

Як вже було зазначено раніше, немає уніфікованого підходу, як організувати роботу з персональними даними, бо кожна установа чи організація має свою специфіку діяльності. Але є базові вимоги та процедури, передбачені законом та міжнародними стандартами, які необхідно впровадити для захисту інформації. До основних організаційних заходів можна віднести:

- ◊ загальний аналіз діяльності у сфері обробки персональних даних;
- ◊ оцінка ризиків щодо порушення законодавства;
- ◊ розробка внутрішньої документації;
- ◊ упорядкування процедур передачі персональних даних, зокрема транскордонної;
- ◊ призначення та професійна підготовка відповідальної особи;
- ◊ впровадження правил внутрішнього контролю за обробкою персональних даних.

У цьому розділі буде надано відповіді, як на практиці потрібно реалізовувати ці та інші заходи з обробки персональних даних.

ЯК ЗДІЙСНЮВАТИ АНАЛІЗ ДІЯЛЬНОСТІ У СФЕРІ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ?

Внутрішній аудит необхідний для того, щоб установа могла відповісти на питання, чи забезпечено належний захист персональних даних. Зокрема, чи відповідають процеси, політики й документи положенням законодавства. Це дозволяє вчасно виявити проблеми та мінімізувати можливі негативні наслідки.

Є випадки, коли працівники установи або організації не можуть пояснити, з якою метою збирають та обробляють персональні дані, а також, як використовують цю інформацію та які заходи щодо її безпеки застосовують. Якщо немає загального розуміння, як відбувається увесь процес обробки інформації, тоді є підстави вважати, що це відбувається неконтрольовано. Будь-яка установа чи організація повинна бути спроможна відповісти, щонайменше, на такі питання:

	Питання	Відповіді для аналізу діяльності
1	Які завдання та повноваження установи у контексті обробки персональних даних?	Чіткий перелік положень законодавства чи інших документів, які надають право збирати персональні дані конкретній установі (або її структурному підрозділу).
2	Яка правова основа для збору та подальшої обробки персональних даних?	Перелік підстав для збору персональних даних, відповідно до Закону України «Про захист персональних даних» та законодавства, що регулює діяльність конкретної установи.
3	Які види та категорії персональних даних збираються?	Перелік видів та категорій даних. Це дає змогу систематизувати інформацію та обрати необхідні рівні захисту. Також важливо зазначити категорії осіб, чиї персональні дані збираються. Перелік та диференціація цільових груп. надзвичайно важлива, оскільки можуть застосовуватися різні заходи безпеки інформації. Наприклад, якщо збираються персональні дані дитини.
4	Які цілі для обробки персональних даних?	Необхідно вказати конкретні цілі (їх може бути декілька) для збору персональних даних.
5	З яких джерел збирається інформація?	Перелік усіх можливих джерел збору інформації, включаючи навіть ті, що є неформальними. Наприклад, коли працівники державних установ збирають персональні дані з соціальних мереж або за допомогою онлайн додатків (у такому випадку необхідно обґрунтувати законність використання такого джерела інформації).
6	Які процеси застосовуються до обробки персональних даних?	Зазначити перелік усіх процедур, що виконуються з персональними даними, наприклад: збір, реєстрація, накопичення, поширення, передача тощо. Необхідно описати усі ці процеси та провести оцінку щодо відповідності закону.
7	Яка форма обробки персональних даних?	Наприклад, паперова, автоматизована або змішана.

	Питання	Відповіді для аналізу діяльності
8	Які інформаційні системи, ресурси та програми залучені у процес обробки персональних даних?	Треба вказати: назву інформаційної системи/реєстру; документ, що підтверджує право власності та/або користування та документ, що підтверджує спроможність інформаційної системи забезпечити захист інформації[1].
9	Чи забезпечено захист персональних даних в інформаційних системах?	Вказати, які саме інциденти безпеки установа готова попередити/реагувати. Наприклад, запобігання витоку, знищенню, перекрученню, копіюванню, несанкціонованому блокуванню персональних даних у телекомунікаційних мережах та інформаційних ресурсах тощо.
10	Де накопичується та зберігається інформація?	Вказати повний перелік можливих інформаційних ресурсів, де зберігається інформація (сервери, хмарні технології тощо).
11	Які терміни зберігання персональних даних?	Строки та нормативні акти, що регулюють порядок зберігання персональних даних.
12	Де зберігається інформація?	Локалізація персональних даних (наприклад, стаціонарний сервер, хмарні сховища тощо, місце або країна розташування). А також важливо зазначити, хто власник системи[2].
13	Хто бере участь в обробці персональних даних та має доступ до них?	Перелік посадових осіб, які беруть участь в обробці та мають доступ до персональних даних. Зокрема, важливо зазначити їх повноваження щодо роботи з персональними даними.
14	Які внутрішньо-розпорядчі документи регулюють процес обробки персональних даних?	Перелік положень, інструкцій, наказів та інших правил, які регулюють процеси обробки персональних даних та їх безпеку.

1 Відповідно до вимог нормативних документів з технічного захисту інформації.
2 Власник системи — фізична або юридична особа, якій належить право власності на систему.

	Питання	Відповіді для аналізу діяльності
15	Який порядок доступу до персональних даних з боку третіх осіб?	Опис відповідних правил чи інструкцій щодо процедур передачі персональних даних.
16	Як відбувається транскордонна передача або обмін персональними даними? (якщо здійснюється така)	Вказати перелік держав або міжнародних організацій, куди передаються персональні дані. Адреси іноземних суб'єктів відносин та опис здійснених заходів щодо належного захисту інформації при передачі за кордон. Окремо опис заходів, які, відповідно до договору з володільцем персональних даних, вжито іноземним суб'єктом відносин щодо гарантій захисту.
17	Яким чином забезпечуються права суб'єктів персональних даних?	Опис способів та засобів комунікації з суб'єктами персональних даних. Порядок забезпечення прав людини відповідно до Закону України «Про захист персональних даних».
18	Чи призначена відповідальна особа за обробку персональних даних (або окремий структурний підрозділ)?	Перелік відповідальних осіб та їхні посадові обов'язки, повноваження та напрямки відповідальності щодо захисту та обробки персональних даних.
19	Який рівень підготовки персоналу з питань захисту персональних даних?	Перелік та кількість заходів, які проведені для персоналу протягом певного періоду. Зокрема, які питання висвітлювалися. Періодичність проведення навчальних заходів.
20	Коли персональні дані підлягають видаленню або знищенню?	Треба вказати конкретні підстави для видалення персональних даних. Наприклад, після закінчення строку зберігання; видання відповідного припису Уповноваженого Верховної Ради України з прав людини; набрання законної сили рішення суду тощо. Прописати процедуру здійснення контролю строків зберігання.
21	У який спосіб знищуються/ видаляються персональні дані?	Потрібно описати визначену процедуру видалення персональних даних. Наприклад, створюється спеціальна комісія, яка складає відповідний акт; інформація видаляється автоматично з систем або вручну; передається в архів тощо. Якщо інформація видаляється з інформаційних систем — необхідно передбачити такий спосіб видалення, що виключає можливість відновлення персональних даних.

Базовий аналіз діяльності установи (або її окремого структурного підрозділу) дасть змогу визначити проблеми та розробити загальну стратегію роботи з персональними даними. Якщо установа має багато різних структурних підрозділів, то такий опитувальник можна розіслати кожному окремо, а потім узагальнити інформацію.

ЯК ОЦІНЮВАТИ РИЗИКИ ПІД ЧАС ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ?

Відповідно до положень, визначених у міжнародних стандартах[1], суб'єкти, які здійснюють обробку персональних даних, повинні проводити оцінку ризиків[2] для того, щоб передбачити ситуації, що можуть мати загрози для прав і свобод людини ще до початку їх настання.

Такі вимоги також зазначені й у європейському законодавстві[3] та інших країн світу.

Тобто кожна установа повинна розробити свою методологію, яка буде враховувати специфіку її діяльності та потреби в оцінки ризиків. Загалом, головна мета цього процесу — відповісти на питання:

- які існують загрози?
- які джерела їх виникнення?
- які наслідки можуть настати?
- що потрібно зробити, щоб їх усунути?

Це особливо потрібно, коли, наприклад: запускається новий проєкт, з'являються нові цілі та збирається інший вид персональних даних; змінюється програмне забезпечення за допомогою якого здійснювалась обробка інформації тощо. Крім цього, провести оцінку варто у наступних ситуаціях:

1. Переведення паперових записів або документів в електронні.
2. Об'єднання декількох баз персональних даних в одну (що не рекомендується робити, оскільки агрегація баз даних може нести багато загроз).
3. Створення нових баз персональних даних або впровадження нових процесів обробки інформації.

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

2 Під поняттям «ризик» мається на увазі сценарій, що описує подію, її причини та наслідки. А також оцінюється з точки зору складності та ймовірності.

3 Необхідність проведення оцінки впливу на захист даних, або ще англ. Data Protection Impact Assessment (DPIA), передбачена статтею 35 Загального регламенту захисту даних (GDPR/ Регламент) та іншими документами.

У європейському законодавстві оцінка впливу на захист персональних даних, або ще Data Protection Impact Assessment (надалі — DPIA) — процедура, передбачена статтею 35 GDPR, а також іншими документами, які визначають міжнародні стандарти безпеки даних[1]. DPIA — це процес, покликаний допомогти аналізувати, виявляти й мінімізувати ризики для персональних даних під час їх обробки. Невиконання DPIA, коли це обов'язково необхідно, може привести до притягнення до відповідальності у вигляді штрафу. Наприклад, пунктом 84 GDPR визначено, що: «.....контролер повинен нести відповідальність за проведення оцінювання впливу на захист персональних 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[2]».

1 «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».

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

4. Залучення нових сторін на підставі договору. Наприклад, реалізація проєктів з використанням сторонніх постачальників.
5. Додавання нових функцій в наявний продукт або послугу.

Часто керівники установ вважають, що вони без додаткових методологій розуміють повну картину щодо роботи з персональними даними та знають про ймовірні ризики. Але вже є багато прикладів, коли можна було б уникнути небезпечних ситуацій, якби керівники установ чи організацій були б краще освічені щодо роботи з персональними даними. Ризик завжди має причинно-наслідковий зв'язок, тому аналіз включає розгляд всіх можливих сценаріїв щодо наслідків обробки персональних даних.

У чинному законодавстві немає зобов'язань відносно типів обробки, які підлягають оцінці, але, з огляду на європейські стандарти, які мають бути орієнтиром для України, такий перелік є. Так, наприклад, у статті 35 (3) GDPR визначено три типи обробки, для яких завжди потрібно DPIA:

Систематичне й масштабне профілювання фізичних осіб:

(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».

Широкомасштабне опрацювання спеціальних категорій персональних даних:

(B) «широкомасштабного опрацювання спеціальних категорій даних, вказаних у статті 9 (1), та персональних даних про судимості і кримінальні злочини, вказані в статті 10».

Громадський моніторинг:

(C) «систематичного та широкомасштабного моніторингу зони, що знаходиться у відкритому доступі[1]».

1 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

Відповідно до статті 29 GDPR особа, що збирає персональні дані (контролер) встановлює відповідні інструкції для їх обробки та захисту. Робоча група органів ЄС у сфері захисту персональних даних опублікувала[1] керівні принципи, які можуть виступати як індикатори обробки з високим ступенем ризику, наприклад, коли:

- ◊ обробка персональних даних здійснюється за допомогою інноваційних технологій, зокрема штучного інтелекту (AI);
- ◊ застосовується автоматизоване прийняття рішень;
- ◊ обробка медичних, біометричних або генетичних даних (окрім випадків, коли це здійснюється медичними працівниками для надання допомоги людині);
- ◊ обробка, яка включає відстеження геолокації або поведінки людини, включаючи, крім іншого, онлайн-середовище;
- ◊ обробка персональних даних дитини, зокрема в маркетингових цілях;
- ◊ якщо обробка персональних даних має такий характер, що витік цієї інформації може нести загрозу для здоров'я або фізичної безпеки людей[2].
- ◊ застосовується масштабне профілювання людей[3].

Процес оцінки ризиків має складатися з певних етапів.

Для початку потрібно проаналізувати напрямки роботи установи в цілому (або її окремого структурного підрозділу). Раніше вже було запропоновано список питань, які можуть допомогти проаналізувати діяльність у даній сфері (див. «Як здійснювати аналіз діяльності у сфері обробки персональних даних?».

Далі — визначити для чого потрібно проводити дану процедуру, адже від мети аналізу буде залежати сценарій та зміст його методології. А також те, скільки

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

2 Приклади операцій, що вимагають DPIA та які критерії є високим ризиком в поєднанні з іншими, що «можуть призвести до високого ризику», можна ознайомитися: 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/

3 Профілювання означає будь-яку форму автоматизованої обробки персональних даних, що складається з використання особистої інформації людини для оцінки певних аспектів, наприклад, що стосуються її роботи, соціального статусу, здоров'я, особистих уподобань, місцезнаходження, переміщення тощо

треба часу, ресурсів та який очікуваний результат. Скажімо, установа запускає новий цифровий продукт й мета буде — оцінити ризики під час його використання. Тоді складається методологія оцінки, яка буде сконцентрована саме цій діяльності. Коли вже є детальний профіль суб'єкта (тобто, конкретної установи), визначена ціль та методологія аналізу, наступає етап — безпосередньої оцінки ризиків.

Результати оцінки ризиків варто задокументувати[4]. Як вже зазначено вище, у чинному законодавстві немає прямих вимог щодо процедури оцінки ризиків, тому кожна установа може самостійно визначати очікувані результати свого аналізу. Головне, щоб в організаційній діяльності установи були передбачені такі процеси, які стануть частиною її ефективної системи внутрішнього контролю у сфері обробки персональних даних.

4 Посібник «Аналіз ризиків під час обробки персональних даних: що важливо знати?» Детальніше з методологією оцінки ризиків можна ознайомитися за посиланням: https://decentralization.gov.ua/uploads/library/file/774/Posibnyk_ocinka-ryzykiv-ZPD.pdf

ПРИКЛАД СТРУКТУРИ РЕЗУЛЬТАТІВ ЗАГАЛЬНОГО ЗВІТУ ОЦІНКИ РИЗИКІВ[5]

	Питання	Відповіді для аналізу діяльності
1	Зміст	Зміст звіту про оцінку ризиків.
2	Коротке резюме та окремі застереження	Інформація про установу (або її структурний підрозділ, підпорядковану установу, де здійснюється оцінка ризиків у сфері захисту персональних даних), її діяльність, правові підстави, команду, місцезнаходження, можливо, ще персональні дані, що стало передісторією для проведення оцінки ризиків. Наприклад, відбувся інцидент безпеки персональних даних, який привів до необхідності аналізу певних процедур з обробки персональних даних. Також важливо зазначити окремі застереження. Наприклад, попередні скарги, звернення тощо від суб'єктів персональних даних. Якщо раніше вже проводилась оцінка ризиків. Короткі тези щодо висновків та рекомендацій.
3	Вимоги законодавства та особливі вимоги	Перелік норм законів, стандартів, міжнародних правил, внутрішніх документів тощо. Також можуть бути особливі вимоги з боку уряду, рекомендації контролюючих органів у даній сфері або рішення суду тощо.
4	Предмет оцінки	Конкретна область аналізу (сервіси, послуги, вид діяльності, технології тощо).
5	Мета	Для чого необхідно провести оцінку ризиків (наприклад, впровадження нового цифрового продукту чи сервісу, зміна в процесах обробки персональних даних тощо).
6	Основні завдання	Процеси обробки персональних даних підлягають оцінці (наприклад, збір, передача, використання, зберігання, видалення, знищення або весь цикл обробки даних).
7	Вид та категорія персональних даних, що обробляються.	Перелік персональних даних, що збирає організація (саме в частині оцінювання).

5 Цей приклад не є шаблоном, а скоріше демонстрація можливого сценарію цього процесу.

	Питання	Відповіді для аналізу діяльності
8.	Особливі категорії персональних даних	Перелік та опис персональних даних, які несуть особливий ризик (в частині оцінювання).
9.	Процеси обробки, що підлягають оцінці	Перелік та опис процесів обробки персональних даних, зокрема тих, що несуть особливий ризик. Оцінка цих процесів з точки зору ризику та категоризація за рівнем загроз.
10.	Законна підстава та цілі обробки	Перелік підстав по кожному виду обробки та цілей. Співвідношення пропорційності та сумісності цілей.
11.	Локалізація	Місцезнаходження інформації: де обробляється та зберігається.
12.	Технічний аналіз та моделювання сценаріїв	Аналіз технічного захисту систем, якщо здійснюється автоматизована обробка персональних даних.
13.	Категорії суб'єктів персональних даних	Важливо зазначити категорії суб'єктів та визначити диференціацію можливих для них загроз (наприклад, через вік, соціальний статус, стать, уподобання або переконання тощо).
14.	Доступ даних третіх осіб	Опис підстав, мети та умов передачі персональних даних третім особам. А також, їх перелік. Також у звітах можуть вказуватися, хто є найчастішим серед запитувачів інформації та з якої причини. Наприклад, може виявитися, що до установи (або конкретного структурного підрозділу) часто надходять адвокатські запити чи органів правопорядку про надання доступу до певних видів та категорій персональних даних. Це може бути сигналом для наявних або потенційних ризиків.

	Питання	Відповіді для аналізу діяльності
15.	Розпорядники інформації (особи, кому передається інформація згідно з законом, договором чи іншим актом)	Перелік розпорядників, мета, підстави та умови передачі персональних даних. Наприклад, деталі щодо договірних відносин з розпорядниками персональних даних: цілі роботи, відповідно до яких отримана згода на обробку персональних даних; перелік дій (операцій) з персональними даними, які здійснюються розпорядником у рамках договору; обов'язки щодо конфіденційності інформації.
16.	Транскордонна передача персональних даних	Країна, цілі, умови та підстави для транскордонної передачі.
17.	Зберігання та видалення персональних даних	Окремої уваги заслуговує питання як, де та який строк зберігається інформація. Умови та процедури видалення.
18.	Матриця оцінки ризиків	Визначення причинно-наслідкового зв'язку між ймовірним ризиком та наслідками, що можуть настати по окремо кожному процесу.
19.	Висновки та рекомендації	Результати оцінки ризиків. Детальний опис заходів щодо зменшення або усунення ризиків. Бажано сформувати рекомендації щодо реагування по кожному окремому процесу/ризику.

З цього прикладу також можна зробити висновки, що значно спрощується процедура оцінки ризиків, якщо вже є детальний аналіз діяльності установи у даній сфері.

ЯКІ НЕОБХІДНІ ВНУТРІШНІ ДОКУМЕНТИ?

Загальний процес обробки персональних даних передбачає різні напрямки роботи, наприклад, окремо збір інформації, використання, передача, поширення, видалення тощо. Часто на практиці ці завдання можуть виконувати різні людини або навіть структурні підрозділи в межах діяльності однієї установи. Для того, щоб контролювати цей процес та здійснювати обробку персональних даних законно й прозоро, потрібно упорядкувати цю роботу за допомогою відповідних внутрішньо-розпорядчих документів.

До переліку таких положень можна віднести:

1. Політику щодо обробки персональних даних (або ще Політика приватності), де мають бути визначені загальні правила роботи з персональними даними. Часто, в державних органах Політику приватності називають Порядком обробки персональних даних. Текст цього документа має бути опублікований на офіційному сайті установи або доступний для перегляду іншим способом[6].
2. Реєстр обробки персональних даних.
3. Загальна внутрішня інструкція роботи з персональними даними, де визначені чіткі вимоги для персоналу, залежно від їхніх повноважень щодо роботи з даними. Зокрема, правила розгляду запитів суб'єктів, чиї дані обробляються[7]. У деяких країнах світу організації або галузеві асоціації приймають спеціальні кодекси, де визначаються правила поведінки під час роботи з конфіденційною інформацією[8]. Це є важливою частиною не тільки для внутрішнього контролю обробки персональних даних, а й для репутаційної складової.
4. Правила здійснення внутрішнього контролю за процесами обробки персональних даних.
5. Правила роботи зі знеособленими персональними даними. Якщо в установі є необхідність у знеособлені великого обсягу персональних даних на постійній основі, тоді бажано для цього розробити окремий порядок. Наприклад, коли установа знеособлює дані з комплексних міських систем відеоспостереження, на практиці для цього може бути призначена окрема посадова особа.
6. Перелік місць зберігання матеріальних носіїв персональних даних. Буде доцільно розробити окремий документ, якщо персональні дані зберігають не в одному місці або навіть країні (у разі, якщо таке допустимо).
7. Посадові інструкції осіб, відповідальних за організацію обробки персональних даних, де буде також міститися зобов'язання про нерозголошення персональних даних.
8. Правила щодо передачі персональних даних третім особам або їх поширення. У тому числі документи, які стосуються порядку транскордонної передачі персональних даних (у разі, якщо така здійснюється).

Цей перелік не є вичерпним. Зміст необхідної документації залежить від функцій конкретної установи, а також вимог законодавства, що регулюють її діяльність.

6 Документ, розроблений володільцем або розпорядником персональних даних, у якому описано весь процес обробки персональних даних.
7 Чіткі внутрішні правила щодо організації та забезпечення усього циклу обробки даних (збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення тощо).
8 Наприклад Всеукраїнська Асоціація Центрів надання адміністративних послуг у 2020 році прийняла Кодекс поведінки з обробки та захисту персональних даних у ЦНАП.

ЩО ТАКЕ РЕЄСТР ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ?

Серед переліку необхідних внутрішніх документів — реєстр обробки персональних даних. Він являє собою своєрідну дорожню карту цілісного потоку інформації, яка наочно має показувати увесь процес її обробки (наприклад, від збирання до видалення)[9]. Реєстр може складатися в будь-якій формі та вигляді, головне — щоб у ньому містилася інформація про:

1. правові підстави та джерела збору персональних даних;
2. цілі обробки персональних даних;
3. види та категорії персональних даних, що збираються;
4. перелік осіб, які мають доступ до персональних даних та беруть участь в їх обробці;
5. перелік третіх осіб, кому було або буде розкрито персональні дані, включаючи треті країни або міжнародні організації, а також законні підстави та цілі надання інформації.
6. строки зберігання та видалення персональних даних;
7. організаційні заходи безпеки персональних даних.

У разі передачі персональних даних на вимогу третіх осіб у реєстрі фіксується:

- ◊ особа (ім'я, посада та організація/установа), що запитує інформацію;
- ◊ вид та категорія персональних даних;
- ◊ повноваження, мета й підстави запиту третьої особи;
- ◊ дата, час та спосіб передачі інформації;
- ◊ ім'я та/або посада особи, яка передала персональні дані.

Це легко зробити, коли вже було попередньо проведено загальний аналіз діяльності установи у даній сфері (див.вище). Не варто плутати ці два документи, бо перший надає загальну картину, як здійснюється робота з персональними даними, а у реєстрі постійно фіксується будь-яка з ними дія. Він дозволяє контролювати обробку інформації, знати, хто мав доступ, кому було передано тощо.

Коли в установі є реєстр, це дозволяє побачити, що відбувається у цій сфері. Можна швидко перевірити або оновити інформацію, наприклад, для контролю строку зберігання, чи здійснити перевірку щодо наявності надлишкових даних тощо. Або якщо є запит від особи про надання інформації про обробку її персональних даних.

Отже, основна мета реєстру — упорядкувати весь цикл обробки персональних даних та відповісти на питання: «яка проводилась робоза з персональними даними, скажімо, годиною раніше?».

9 У європейському законодавстві, а саме стаття 30 GDPR встановлює обов'язок вести такий реєстр для кожного контролера та процесора.

ЯКИЙ ПОРЯДОК ДОСТУПУ ДО ДАНИХ З БОКУ ТРЕТІХ ОСІБ?

Порядок передачі персональних даних третім особам займає одне із важливих питань, бо часто саме у цьому процесі фіксуються серйозні порушення законодавства у цій сфері. Передача, поширення або оприлюднення інформації про особу може завдати шкоди її правам і свободам.

Як вже було зазначено вище, у статті 19 Конституції України визначено, що ніхто не може бути примушений робити те, що прямо не передбачено законодавством. Органи державної влади та їх посадові особи зобов'язані діяти лише на підставі, в межах повноважень та у спосіб, що передбачені Конституцією та законами України. З огляду на це положення, надавати інформацію на такий запит можна лише за наявності повноважень, законної підстави й обґрунтованої мети та у спосіб, передбачений законом.

Передача персональних даних третім особам здійснюється на офіційний запит, у якому мають бути зазначені:

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

Строк вивчення запиту не може перевищувати 10 робочих днів з дня надходження. Протягом цього строку необхідно повідомити особу, яка подала запит, чи буде його задоволено або чому запитувана інформація не підлягає наданню. Запит розглядається протягом 30 календарних днів з дня його надходження, якщо інше не передбачено законом.

Порядок передачі персональних даних третім особам займає одне із важливих питань, бо часто саме у цьому процесі фіксуються серйозні порушення законодавства у цій сфері. Передача, поширення або оприлюднення інформації про особу може завдати шкоди її правам і свободам.

Відстрочення доступу до персональних даних третіх осіб допускається у разі, якщо дані не можуть бути надані протягом 30

календарних днів з дня надходження запиту. При цьому, загальний термін розгляду не може перевищувати 45 календарних днів[10]. Повідомлення про відстрочення доводиться до відома третьої особи, яка подала запит, у письмовій формі з роз'ясненням порядку оскарження такого рішення.

- У повідомленні про відстрочення зазначаються:
- прізвище, ім'я та по батькові посадової особи;
- дата відправлення повідомлення;
- причина відстрочення;
- строк, протягом якого буде задоволено запит.

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

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

Підставою для відмови, окрім відсутності у запитувача повноважень чи правових підстав для обробки персональних даних, також може бути невідповідність запиту вимогам статті 16 Закону України «Про захист персональних даних», зокрема:

- не зазначення точного переліку суб'єктів, чиї персональні дані запитуються;
- не надання достатніх відомості, що дають змогу ідентифікувати фізичну особу, стосовно якої робиться запит (наприклад, за наданими персональними даними в базі даних / реєстрі знайдено декількох осіб);
- не зазначено точний перелік персональних даних які запитуються (наприклад, якщо запитують будь-які, якими володіє установа).

При прийнятті рішення про надання доступу до персональних даних третім особам необхідно звернути увагу, на відповідність запитуваного переліку персональних даних меті зазначеній у запиті. Отже, отримати можливо саме ті персональні дані, що відповідають зазначеній меті запитувача.

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

Порядок передачі персональних даних правоохоронним органам роз'яснений у листі Представника Уповноваженого Верховної Ради України з прав людини від 28.12.2015 року «Щодо правових підстав передачі персональних даних правоохоронним органам[1]», в якому вказується: «належною підставою для отримання правоохоронними органами доступу до персональних даних в рамках кримінального провадження є ухвала слідчого судді, суду про тимчасовий доступ до речей і документів. Усі інші запити на доступ до персональних даних мають розглядатися індивідуально з огляду на повноваження запитувача, підстави запиту, обсяг запитуваної інформації тощо».

1 Офіційний сайт Уповноваженого Верховної ради України з прав людини.

ЯК ЗДІЙСНЮЄТЬСЯ ТРАНСКОРДОННА ПЕРЕДАЧА ПЕРСОНАЛЬНИХ ДАНИХ?

Співробітництво з іноземними суб'єктами відносин, пов'язаних із персональними даними, регулюється Конституцією України, Законом України «Про захист персональних даних», іншими нормативно-правовими актами та міжнародними договорами. Якщо міжнародним договором України, згода на обов'язковість якого надана Верховною Радою України, встановлено інші правила, ніж ті, що передбачені законодавством України, то застосовуються правила міжнародного договору України.

Передача персональних даних іноземним суб'єктам відносин здійснюється лише за умови забезпечення відповідною державою належного захисту персональних даних у випадках, встановлених законом або міжнародним договором України.

Держави-учасниці Європейського економічного простору, а також держави, які підписали Конвенцію Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних, визнаються такими, що забезпечують належний рівень захисту персональних даних.

Кабінет Міністрів України визначає перелік держав, які забезпечують належний захист персональних даних. Персональні дані не можуть поширюватися з іншою метою, ніж та, з якою вони були зібрані. Разом з тим, можуть передаватися іноземним суб'єктам відносин, пов'язаних з персональними даними, також у разі:

1. надання суб'єктом персональних даних однозначної згоди на таку передачу;
2. необхідності укладення чи виконання правочину між володільцем персональних даних та третьою особою-суб'єктом персональних даних на користь суб'єкта персональних даних;
3. необхідності захисту життєво важливих інтересів суб'єктів персональних даних;
4. необхідності захисту суспільного інтересу, встановлення, виконання та забезпечення правової вимоги;
5. надання володільцем персональних даних відповідних гарантій щодо невтручання в особисте і сімейне життя суб'єкта персональних даних[11].

Разом з тим, треба звернути увагу, що в чинному законодавстві немає терміну «транскордонна передача персональних даних», але держава Україна є учасницею міжнародних відносин та договорів, які були ратифіковані Верховною Радою України, які є обов'язковими до виконання. Це означає, що регламентуючи експорт персональних даних за межі країни необхідно опиратися на європейські та міжнародні стандарти, які, зокрема Україна зобов'язалася виконувати в рамках Угоди про асоціацію з ЄС[12].

11 Стаття 29 «Міжнародне співробітництво та передача персональних даних».
12 Угода про асоціацію між Україною та Європейським Союзом, Європейським співтовариством з атомної енергії та їх державами-членами, з іншого боку (Угоду ратифіковано із заявою Законом № 1678-VII від 16.09.2014 року).

Транскордонна передача передбачає процес надання персональних даних третій країні або міжнародній організації. Передача даних іноземним суб'єктам відносин має здійснюватися лише за умови забезпечення належного рівня їх захисту. Держави-учасниці Європейського економічного простору, а також, які підписали Конвенцію 108, визнаються такими, що забезпечують відповідний рівень захисту персональних даних[13].

Щодо інших держав, то Кабінет Міністрів України (надалі — КМУ) постановою від 16 серпня 2022 року № 910 встановив такий перелік країн[14]. Це було необхідно для забезпечення громадян України використання їхніх електронних документів або передачі їх електронних копій; отримання публічних послуг за межами України. Персональні дані за бажанням особи можуть засобами Порталу Дія передаватись іноземним суб'єктам відносин, пов'язаним з персональними даними, в державах, що забезпечують належний їх захисту.

Міністерство цифрової трансформації забезпечило підключення інформаційних систем до іноземних суб'єктів відносин, пов'язаних з персональними даними, держав, зазначених у переліку, до Єдиного державного вебпорталу електронних послуг згідно з Положенням про Єдиний державний вебпортал електронних послуг, затвердженим постановою КМУ від 4 грудня 2019 року № 1137.

Отже, кожна установа, яка має намір здійснювати транскордонну передачу інформації, повинна укласти окремий договір про взаємний її захист. Ці гарантії мають бути передбачені у положеннях міжнародних договорів про співробітництво або додатках до них. Необхідно визначати коло суб'єктів персональних даних, до яких буде застосовуватися договір, обсяг персональних даних, що оброблятимуться в межах його виконання, порядок їх обробки, строк зберігання та процедури видалення.

Також важливо врахувати положення Директиви 2016/680, де передбачена заборона профілювання на основі персональних даних, бо такі дії в результаті можуть призвести до дискримінації фізичних осіб[15]. Отже, транскордонна передача персональних даних без наявності законних підстав, повноважень та визначених чітких процедур забезпечення належних гарантій їх захисту, заборонена.

13 Перелік держав, які підписали зазначену Конвенцію, розміщено на офіційному вебсайті Ради Європи. Режим доступу: https://www.coe.int/en/web/conventions/full-list?module=signatures-by- treaty&treatynum=108.
14 Ознайомитися з переліком можна на офіційному сайті Кабінету Міністрів України.

15 Рекомендації Уповноваженого Верховної Ради України з прав людини щодо забезпечення захисту даних під час укладання Україною міжнародних договорів, які передбачають транскордонний обмін даними. Режим доступу: https://ombudsman.gov.ua/storage/app/media/transkordonna-peredacha-personalnyh-danyh.pdf

ЧИ МОЖНА ВИКОРИСТОВУВАТИ РЕЄСТРАЦІЙНІ ФОРМИ ЗА ДОПОМОГОЮ СЕРВІСУ GOOGLE?

Google форми стали одним із найпростіших способів зареєструвати учасників на заходи, навчання, співбесіди та здійснити опитування тощо. Проте більшість із них не відповідають вимогам законодавства у сфері захисту персональних даних та можуть становити загрозу для осіб, які заповнюють такі форми.

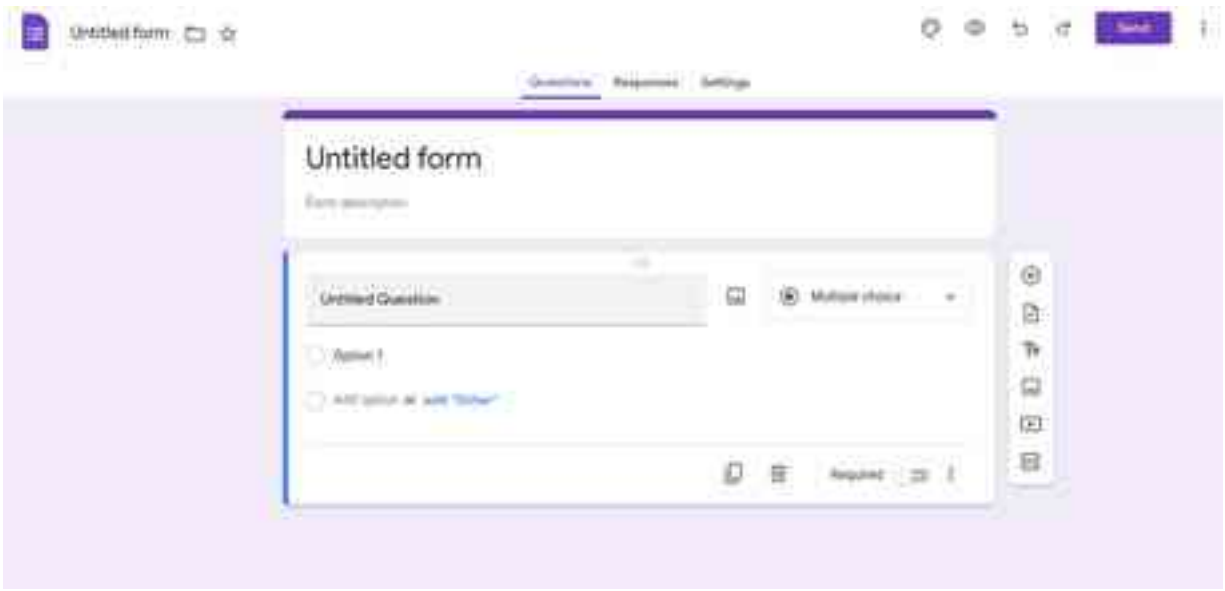
Перш за все, за допомогою сервісу Google, який дозволяє створювати спеціальні форми, збирається значна кількість особистих даних, серед яких можуть бути й вразливі персональні дані. За допомогою Google-форм переважно збирається така інформація: прізвище та ім'я особи, її вік, стать, сферу діяльності, дані про освіту, професію; рівень володіння знаннями у тій чи іншій сфері; також ще може запитуватися політичні уподобання та приналежність до певних соціальних груп населення, етнічних або національних меншин. Це можна назвати профілюванням осіб. Така обробка даних несе високий ризик для прав і свобод людини.

Навіть якщо надається інформація про цілі збору персональних даних (наприклад, для організації просвітницького заходу), то часто не зрозуміло, чому запитується саме такий вид та категорія (наприклад, в гугл-формах можна побачити запитання про стан здоров'я людини, точну адресу проживання). Тобто, збирається надлишковий обсяг персональних даних, який не відповідає визначеним цілям їх використання[16].

Органи державної влади обробляють персональні дані на підставі дозволу, наданого законом виключно для здійснення повноважень. Це відповідає статті 19 Конституції України. У разі якщо підставою обробки персональних даних є дозвіл, наданий законом, у законодавстві визначається мета обробки, обсяг персональних даних, які може обробляти окремий орган, а також джерела з яких дані можуть отримуватися або надалі передаватися третім особам. Те ж стосується і такої підстави обробки персональних даних, як необхідність виконання обов'язку володільця персональних даних, який передбачений законом.

Будь-яке використання цифрових технологій (або пристроїв чи мобільних додатків), з боку органів влади має бути дозволено на державному рівні, пройдена процедура сертифікації з наданням рекомендацій відповідальних служб щодо безпеки інформації.

16 Згідно з частиною три статті 2 Закону України «Про захист персональних даних» володілець даних передусім має чітко визначити мету обробки, встановити обсяг цих даних відповідно до мети та процедури їх обробки. Разом із тим, відповідно до частини третьої статті 6 Закону склад і зміст даних мають бути відповідними, адекватними та ненадмірними відносно визначеної мети обробки.



Крім того, слід звернути увагу на наступне:

- ◊ сервери компанії Google, на яких фактично зберігаються персональні дані зібрані через Google форми знаходяться за межами України. Тобто, використання Google форм призводить до транскордонної передачі, про яку йшлося у попередньому розділі;
- ◊ у більшості випадків, опитування чи реєстраційні форми розміщенні на вебсайтах державних органів чи місцевого самоврядування створюються працівниками таких органів зі своїх приватних аккаунтів. Таким чином, частково обробка персональних даних здійснюється поза контролем згаданих органів, а законність джерела їх отримання (приватний аккаунт працівника) є сумнівною.

Тобто, використання Google форм органами державної влади чи місцевого самоврядування для реєстрації на заходи або проведення опитувань є незаконним. Це має здійснюватись шляхом офіційного листування або з використанням офіційних робочих адрес електронної пошти. Що стосується опитувань, то вони мають проводитись анонімно з використанням офіційних вебсторінок органів державної влади.

ЯКА ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ ЗАКОНОДАВСТВА У СФЕРІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ?

Контроль за додержанням законодавства у цій сфері здійснюють Уповноважений Верховної Ради України з прав людини та суди[17]. Порушення законодавства про захист персональних даних тягне за собою відповідальність, яка передбачена:

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

НАВІЩО ПРИЗНАЧАТИ ВІДПОВІДАЛЬНУ ОСОБУ?

Закон в окремих випадках вимагає[18] призначати відповідальних осіб або навіть структурний підрозділ, який має контролювати процес обробки персональних даних та їх захист. Наприклад, у європейському Регламенті (GDPR) така посада називається — Data Protection Officers (DPO)[19].

Забезпечення захисту персональних даних — це безперервний та систематичний процес. Тобто недостатньо розробити, наприклад, Політику приватності та опублікувати її на офіційному сайті. Має бути створена ефективна система внутрішнього контролю повного циклу обробки персональних даних. Це надає змогу своєчасно виявити й усунути порушення у цій сфері. Призначення відповідальної особи треба оформити відповідним наказом, з яким особа ознайомлюється під підпис. Також інформація про підрозділ чи відповідальну особу направляється Уповноваженому Верховної Ради України з прав людини[20].

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

18 У Законі «Про захист персональних даних» є положення, яке зобов'язує тих, хто збирає та обробляє персональні дані призначити відповідальну особу або, у разі необхідності, структурний підрозділ.

19 Завдання DPO в країнах Європейської економічної зони (ЄЕЗ) базово визначені у статті 39 GDPR.

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

ЯКІ ФУНКЦІОНАЛЬНІ ОБОВ'ЯЗКИ ВИКОНУЄ ВІДПОВІДАЛЬНА ОСОБА?

У законодавстві визначено, що відповідальні особи повинні:

- ◊ інформувати та консультувати володільця або розпорядника персональних даних з питань додержання законодавства про захист персональних даних;
- ◊ взаємодіяти з Уповноваженим Верховної Ради України з прав людини та визначеними ним посадовими особами його Секретаріату з питань запобігання й усунення порушень законодавства про захист персональних даних.
- ◊ Керівництво установи самостійно приймає рішення про призначення відповідальної особи, проте з урахуванням наступних аспектів:
- ◊ уникнення конфлікту інтересів;
- ◊ у відповідальної особи має бути достатньо повноважень для виконання покладених на неї функцій з контролю за обробкою персональних даних.

Ключова роль відповідальної особи — розробка стратегії обробки та захисту персональних даних та контроль за її реалізацією. Тому, до функціональних обов'язків доцільно віднести:

- ◊ аналіз діяльності та контроль за проведенням заходів щодо захисту персональних даних;
- ◊ ведення обліку процесів обробки персональних даних;
- ◊ розробка та підтримання в актуальному стані відповідної внутрішньої документації;
- ◊ здійснення оцінки ризиків та внутрішнього контролю за дотриманням законодавства про захист персональних даних;
- ◊ організація приймання та розгляд звернень (запитів) суб'єктів персональних даних, а також запитів третіх осіб та Уповноваженого Верховної Ради України з прав людини;
- ◊ організація у проведенні службових перевірок за фактами порушень вимог до обробки й захисту персональних даних;
- ◊ підготовку органу до перевірок з боку контролюючих інстанцій та організаційне сприяння здійсненню таких перевірок (підготовку необхідних документів, інформації тощо);
- ◊ взаємодію з Уповноваженим Верховної Ради України з прав людини, іншими державними органами контролю та неурядовими громадськими організаціями у питаннях забезпечення прав, свобод і законних інтересів громадян;
- ◊ дослідження змін, пов'язаних з захистом персональних даних (зміни у законодавстві, інновації, технології тощо).

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

ЯКІ ОБОВ'ЯЗКИ У ПОСАДОВИХ ОСІБ, ЯКІ ЗДІЙСНЮЮТЬ ОБРОБКУ ПЕРСОНАЛЬНИХ ДАНИХ?

Може скластися помилкове уявлення, що відповідальність за обробку та захист інформації несе тільки спеціально призначена особа. Це не так, бо дотримуватися положень закону повинні абсолютно усі працівники, що мають доступ до персональних даних. Тому, у посадових інструкціях службовців, діяльність яких пов'язана з обробкою персональних даних, мають бути визначені обов'язки щодо дотримання законодавства у даній сфері.

Зокрема вони повинні бути спроможні:

- роз'ясняти суб'єкту персональних даних його права у даній сфері;
- вживати заходів щодо забезпечення достовірності оброблюваних персональних даних. За необхідності вносити зміни до персональних даних, які є неповними, застарілими або неточними;
- здійснювати контроль за терміном обробки персональних даних відповідно заявленим цілям. Припиняти обробку, а також забезпечувати їх видалення або блокування за відсутності правових підстав для подальшої роботи з персональними даними;
- надавати доступ, передавати або поширювати персональні дані лише за наявності відповідної правової підстави;
- забезпечувати доступ до персональних даних у встановленому порядку, вести облік (реєстр) у разі розповсюдження персональних даних третім особам.

Конкретний перелік таких обов'язків визначається у кожному конкретному випадку, в залежності від специфіки діяльності працівника.

ЩО ВАЖЛИВО У ПРОФЕСІЙНІЙ ПІДГОТОВЦІ?

Цифрова трансформація системи державного управління спонукає до постійних змін в законодавстві, у тому числі міжнародному, які необхідно впроваджувати у практичну діяльність. Для цього потрібна якісна професійна підготовка не тільки для відповідальних осіб за обробку персональних даних, а усіх хто працює з інформаційними системами або дотичний до них.

Особи, які залучені у процес обробки персональних даних повинні бути ознайомлені з внутрішніми документами та положеннями законодавства з питань захисту інформації та персональних даних. Адже люди не можуть дотримуватися того, чого не знають.

Питання, які повинні розглядатися в рамках професійної підготовки:

- роз'яснення положень національного законодавства та міжнародних стандартів у сфері захисту персональних даних.
- критерії законності обробки даних.
- аналіз діяльності та оцінка ризиків під час обробки персональних даних.
- права суб'єкта персональних даних.
- повноваження, законна підстава та порядок доступу до інформації з боку третіх осіб.
- розробка внутрішньої документації (зміст, процедури та заходи).
- операції з обробки персональних даних, що можуть становити особливий ризик для прав і свобод людини.
- використання інформаційних систем: ведення реєстрів, терміни зберігання, порядок доступу третіх осіб, інформування суб'єктів персональних даних.
- організація безпеки фізичного середовища та інформаційних систем (управління, моніторинг та авторизація доступу, безпека приміщення тощо).
- технічний захист інформації, що містить персональні дані.
- видалення або знищення персональних даних.
- правила внутрішнього контролю та відповідальність.

ЯКІ Є ПРАВИЛА ВНУТРІШНЬОГО КОНТРОЛЮ?

Внутрішній контроль є невід'ємною частиною процесу захисту персональних даних. Основне його завдання — це перевірка усіх процедур щодо законної обробки та безпеки інформації. Контроль необхідний для того, щоб мінімізувати можливі ризики, наприклад, витоку персональних даних, випадкової втрати чи їх знищення.

Основними складовими контролю для перевірки можуть бути:

- ◊ документація, яка регулює усі процедури обробки та захисту персональних даних;
- ◊ призначення відповідальної особи;
- ◊ професійна підготовка та перевірка знань осіб, які залучені у роботу з персональними даними;
- ◊ аналіз діяльності та оцінка ризиків;
- ◊ ведення реєстрів, тобто документування усіх процесів обробки персональних даних (збір, передача, знищення тощо);
- ◊ порядок забезпечення прав суб'єктів, чиї дані обробляються[21];
- ◊ технічний захист інформації, яка обробляється в системах;
- ◊ процедури ідентифікації й аутентифікації в інформаційних системах;
- ◊ перевірка термінів зберігання та видалення персональних даних;
- ◊ проведення резервного копіювання програмних засобів, архівів, журналів, інформаційних активів, які використовуються і створюються в процесі експлуатації інформаційних систем;
- ◊ перевірка процедури поширення та/або передачі персональних даних третім особам тощо.

Питання для внутрішнього контролю можуть формуватися, виходячи зі:

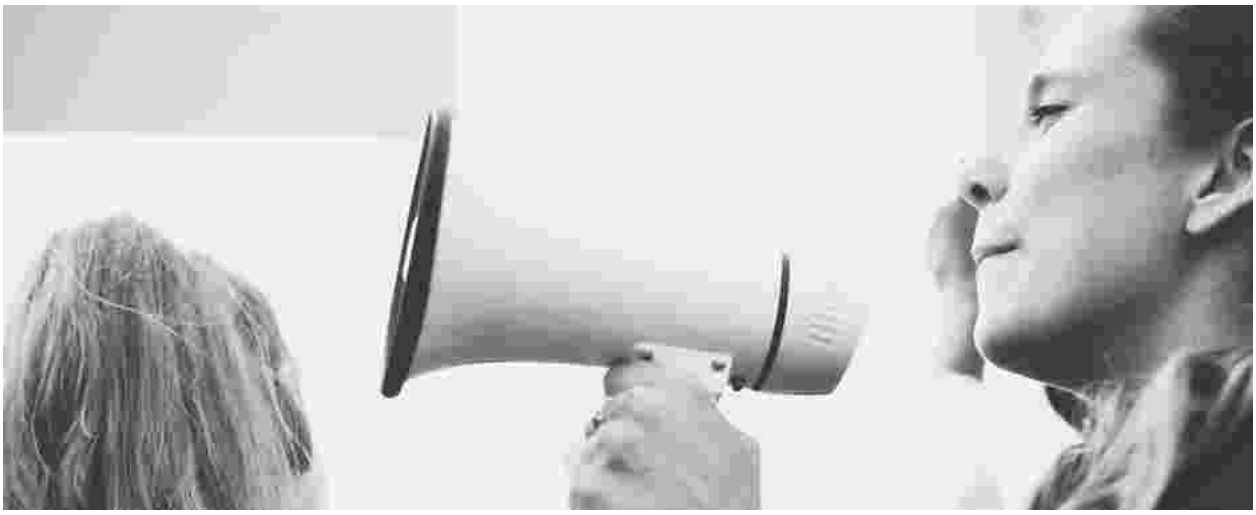
- ◊ специфіки діяльності конкретної установи (наприклад, якщо це визначено законом, що регулює її діяльність);
- ◊ попередніх результатів внутрішнього аналізу діяльності у даній сфері;
- ◊ актів реагування контролюючого органу.

21 Виконання статті 8 Закону України «Про захист персональних даних».

РОЗДІЛ 3

ЗАБЕЗПЕЧЕННЯ ПРАВ СУБ'ЄКТІВ ПЕРСОНАЛЬНИХ ДАНИХ

Кожна особа має особисті немайнові права на свої персональні дані. У законодавстві приділено цьому питанню особливу увагу, адже кожна людина повинна мати можливість контролювати обробку інформації про себе та розуміти усі можливі ризики. Звичайно, є винятки із правил, але вони детально регламентовані у законі.



ЯКІ Є ПРАВА У СУБ'ЄКТА ПЕРСОНАЛЬНИХ ДАНИХ?

- ◊ Знати про джерела збирання, місцезнаходження своїх персональних даних, мету їх обробки, місцезнаходження (перебування) володільця чи розпорядника персональних даних або дати відповідне доручення щодо отримання цієї інформації уповноваженим ним особам, крім випадків, встановлених законом.
- ◊ Отримувати інформацію про умови надання доступу до своїх персональних даних, зокрема інформацію про третіх осіб, яким передаються персональниі дані. Крім випадків, визначених законом.
- ◊ Мати доступ до своїх персональних даних.
- ◊ Отримувати не пізніше як за тридцять календарних днів з дня надходження запиту, крім випадків, передбачених законом, відповідь про те, чи обробляються його персональні дані, а також отримувати інформацію про їх зміст.
- ◊ Пред'являти вмотивовану вимогу із запереченням проти обробки своїх персональних даних, крім випадків, визначених законом.
- ◊ Пред'являти вмотивовану вимогу щодо зміни або знищення своїх персональних даних, якщо ці дані обробляються незаконно чи є недостовірними.
- ◊ На захист своїх персональних даних від незаконної обробки та випадкової втрати, знищення, пошкодження у зв'язку з умисним приховуванням, ненаданням чи несвоєчасним їх наданням, а також на захист від надання відомостей, що є недостовірними чи ганьблять честь, гідність та ділову репутацію фізичної особи.
- ◊ Звертатися зі скаргами на обробку своїх даних до Уповноваженого Верховної Ради України з прав людини або до суду.
- ◊ Застосовувати засоби правового захисту в разі порушення законодавства про захист персональних даних.
- ◊ Вносити застереження стосовно обмеження права на обробку персональних даних під час надання згоди.
- ◊ Відкликати згоду на обробку персональних даних, окрім випадків, коли згода (як правова підстава на збір даних) не застосовується.
- ◊ Знати механізм автоматичної обробки персональних даних.
- ◊ На захист від автоматизованого рішення, яке має для нього правові наслідки[1].

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

ЩО ПЕРЕДБАЧАЄ ПРАВО НА ДОСТУП ДО СВОЇХ ПЕРСОНАЛЬНИХ ДАНИХ?

Статтею 8 Закону України «Про захист персональних даних» передбачено право особи на доступ до своїх персональних даних. Людина може звернутися з питаннями про обробку її особистих даних. Наприклад, серед питань можуть бути:

- з якою метою обробляються персональні дані?
- яке джерело збору інформації (якщо не була отримана безпосередньо від особи)?
- які саме категорії персональних даних?
- кому вони передаються у процесі обробки?
- який термін зберігання та чим визначений такий період?
- чи використовується процес автоматизованого прийняття рішення, включаючи профілювання?

У такому запиті зазначаються:

- прізвище, ім'я та по батькові;
- місце проживання (місце перебування)
- реквізити документа, що посвідчує фізичну особу, яка подає запит (для фізичної особи-заявника)[1].

Доступ особи до персональних даних здійснюється безоплатно[2]. Навіть, якщо така інформація з обмеженими доступом, залишати запит без відповіді не можна. Про заборону у розголошені такої інформації потрібно повідомити, обов'язково вказавши конкретну норму закону, що надає це право.

Комунікація з громадянським суспільством є складним і відповідальним процесом для державних органів. Людина може зробити запит усно або письмово. Тому варто розробити чіткий внутрішній порядок опрацювання таких запитів та звернути увагу, на два аспекти:

По-перше, на практиці часто замість роз'яснення затребуваної інформації, особі просто надається Політика обробки персональних даних, щоб вона самостійно знаходила відповіді на свої питання. Це неправильний підхід, бо необхідно окремо надавати дані, які просить заявник.

По-друге, процедура забезпечення доступу до персональних даних має певні ризики, бо володільці інформації, отримавши такий запит, повинні бути впевнені в тому, що звернувся належний запитувач, а не стороння особа. Це означає, що мають бути передбачені власні процедури ідентифікації запитувача. Водночас такі процедури не повинні необґрунтовано ускладнювати реалізацію права на доступ до своїх персональних даних.

1 Стаття 16 Закону України «Про захист персональних даних».
2 Стаття 19 Закону України «Про захист персональних даних».

ЯКУ ІНФОРМАЦІЮ ТРЕБА НАДАВАТИ НА ВИМОГУ СУБ'ЄКТА ПЕРСОНАЛЬНИХ ДАНИХ?

Згідно з міжнародними стандартами діяльність у сфері захисту персональних даних повинна здійснюватися законно та прозоро[3]. Це означає, що особи, чиї персональні дані збираються, мають право бути поінформовані про процедури обробки та усвідомлювати можливі ризики.

Така інформація має бути зрозумілою й легкодоступною. Це можна зробити, використовуючи різні методи: панелі на вебсайті, через публікацію політик приватності, повідомлення тощо. Разом з тим, людина може звернутися особисто (усно чи письмово) з проханням надати додаткові роз'яснення про:

- повноваження органу стосовно обробки її персональних даних;
- мету, порядок та вид обробки персональних даних;
- джерело збору та місцезнаходження даних;
- порядок передачі персональних даних третім особам;
- умови захисту інформації;
- термін зберігання та порядок видалення;
- іншу інформацію пов'язану з обробкою персональних даних.

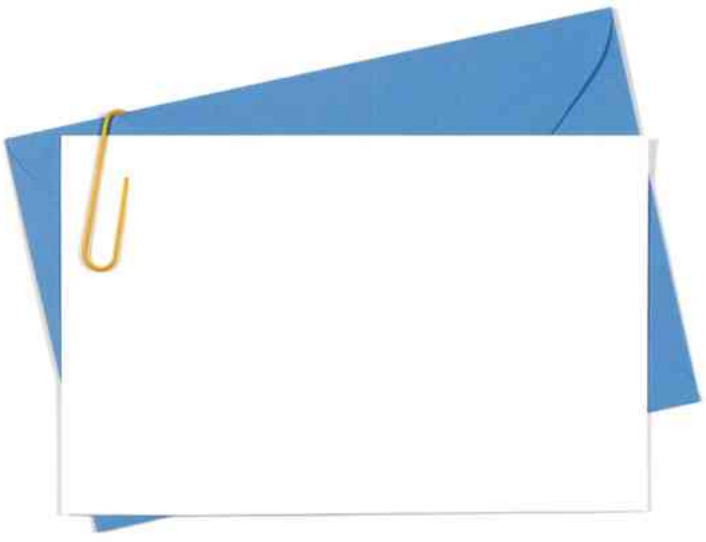
Такий запит має бути задоволено, окрім випадків коли, коли обмеження у наданні такої інформації прямо передбачено законом.

3 Відповідно до міжнародних принципів прозорості, законності та справедливості.

КОЛИ НЕ ПОТРІБНО ПОВІДОМЛЯТИ ОСОБУ ПРО ДІЇ З ЇЇ ПЕРСОНАЛЬНИМИ ДАНИМИ?

Повідомлення, не здійснюються у разі:

- передачіперсональнихданихзазапитами при виконанні завдань оперативно-розшукової чи контррозвідувальної діяльності, боротьби з тероризмом;
- виконання органами державної влади та органами місцевого самоврядування своїх повноважень, передбачених законом;
- здійснення обробки персональних даних в історичних, статистичних чи наукових цілях.



ЩО ОЗНАЧАЄ ПРАВО НА ЗАХИСТ ВІД АВТОМАТИЗОВАНОГО ПРИЙНЯТТЯ РІШЕННЯ?

У зв'язку з розвитком технологічних рішень в системі державного управління, потрібно особливу увагу звернути на право людини на захист від автоматизованого рішення. Особа має право не піддаватися рішенню, яке засноване виключно на автоматизованій обробці, в тому числі профілюванні, що викликає для неї юридичні наслідки або схожим чином суттєво впливає на її життя.

Профілювання та автоматизоване прийняття рішень взаємопов'язані між собою, проте це два окремих інститути зі своїми правилами.

Профілювання означає будь-яку форму автоматизованої обробки персональних даних, що складається з використання особистої інформації людини для оцінки певних аспектів, наприклад, що стосуються її роботи, соціального статусу, здоров'я, особистих уподобань, місцезнаходження, переміщення тощо.[4] Серед поширених прикладів, коли проводиться моніторинг поведінки відвідувачів вебсайту в маркетингових цілях.

Автоматизоване прийняття рішень здійснюється за допомогою комп'ютерних

4 Відповідно до пункту 4 статті 4 GDPR.

систем без втручання людини. Саме відсутність людського втручання є ризиком з точки зору захисту прав та інтересів суб'єктів персональних даних, оскільки програма не знає, як, зрештою, її рішення може вплинути на особу або її життя в цілому. Крім того, при створенні алгоритму не може передбачити абсолютно всі ситуації, які можуть виникнути насправді, що може призвести до помилкового рішення.

- можливість втручання людини для перевірки такого рішення, зокрема на вимогу людини, якої стосувалося прийняте рішення;
- інформування суб'єкта персональних даних про використання технологій;
- надання інформації про механізми та правила, за якими здійснюється прийняття автоматизованого рішення;

У Великобританії в 2000–2014 роках через автоматизоване прийняття рішення відбувся скандал, коли понад 700 співробітників поштової служби отримали покарання, включно з тюремним ув'язненням, за порушення, які вони не скоювали. Згодом було доведено, що комп'ютерна програма припустилася помилок, через які виникли великі грошові недостачі. Тоді тягар доказування невинуватості було перекладено на самих обвинувачених[1]. Презумпція безпомилковості комп'ютера не повинна підміняти собою презумпцію невинуватості людини.

1 Post Office scandal: What the Horizon saga is all about. Режим доступу: https://www.bbc.com/news/business-56718036

Отже, особа має право на захист коли рішення ґрунтуються виключно на автоматичній обробці персональних даних та має правові наслідки або суттєво впливають на особу. Тому, будь-які технологічні рішення, які впроваджуються в систему державного управління або у приватному секторі, повинні передбачати:

- можливість для суб'єкта персональних даних висловити свою думку у разі обробки інформації про нього, а також отримати пояснення щодо такого рішення та оскаржити його[5].

5 Article 29 Working Party, Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679 (2018).

Images used in the publication are by rawpixel.com, Christina Morillo, The Humantra, Ruslan Burlaka on Freepik