М.В. БЕМ,
І.М. ГОРОДИСЬКИЙ

Посольство Великої Британії в Україні
STABILIZATION SUPPORT SERVICES
РАДНИК З ПИТАНЬ ВПО www.radnyk.org
UCU УКРАЇНСЬКИЙ КАТОЛИЦЬКИЙ УНІВЕРСИТЕТ ШКОЛА ПРАВА

ПРАКТИЧНИЙ ПОСІБНИК

СТАНДАРТИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В СОЦІАЛЬНІЙ СФЕРІ

Посібник виданий завдяки фінансовій підтримці Посольства Великої Британії в Україні в рамках проекту "Подолання соціальних наслідків конфлікту на Донбасі та незаконної анексії Криму за допомогою державних структур в Україні та громадянського суспільства", який реалізовує канадська неурядова організація "Stabilization Support Services".

2018

УДК 342.721
ББК Х849 (4укр) 04+Х819(4Укр)011.2-15
АЗ Г 701

Авторський колектив:

Бем М. В., юрист Європейського суду з прав людини, старший викладач кафедри теорії права та прав людини Українського католицького університету

Городиський І. М., член Правління ГО «Львівський центр міжнародного права та прав людини», канд.. юрид. наук, директор Школи права Українського католицького університету

АЗ Г701 **Стандарти захисту персональних даних в соціальній сфері** / М. В. Бем,, *І. М. Городиський*. – Львів: б.в., 2018. - 110 *с.*

Відповідальна за випуск: Олендра Іванна Василівна, експерт ГО «Львівський центр міжнародного права та прав людини»

УДК 342.721
ББК Х849 (4укр) 04+Х819(4Укр)011.2-15

The development and production of the manual was funded by the British Embassy in Ukraine as part of the project. Addressing social consequences of the conflict in Donbas and the illegal annexation of Crimea with support to Ukrainian government bodies and local civil society, which is implemented by Canadian NGO Stabilization Support Services.

Посібник виданий завдяки фінансовій підтримці Посольства Великої Британії в Україні в рамках проекту "Подолання соціальних наслідків конфлікту на Донбасі та незаконної анексії Криму за допомогою державних структур в Україні та громадянського суспільства", який реалізовує канадська неурядова організація "Stabilization Support Services".

ЗМІСТ

ВСТУП

В останні роки, через події на Сході України та економічні труднощі, значно зросла суспільна вага державних органів та інституцій, що функціонують в соціальній сфері. Діяльність Міністерства соціальної політики та органи соціального захисту, а також Міністерства з питань тимчасово окупованих територій та внутрішньо переміщених осіб України є однією з ключових для стабілізації ситуації в країні й вирішення проблем, які стоять перед Україною та її громадянами на цьому етапі.

Одним із актуальних питань, які потребує особливої уваги в розрізі діяльності в цьому напрямку є питання захисту персональних даних осіб, що отримують соціальну допомогу та захист від держави. Події останніх років по всьому світу постійно доводять які великі ризики несе недобросовісна обробка персональних даних. У зв'язку із тим, що зараз в соціальній сфері в Україні обробляються осіб, що постраждали через збройний конфлікт та були змушені покинути тимчасово окуповані території як внутрішньо переміщені особи.

Цей посібник має на меті показати способи та шляхи здійснення належної обробки та захисту персональних даних державними органами, які здійснюють діяльність в сфері соціального захисту, а також принципи і стандарти, на яких має ґрунтуватися робота з обробки та захисту. При його підготовці автори виходили з національного законодавства та європейських стандартів захисту персональних даних, в тому числі новому Регламенту ЄС щодо захисту персональних даних, який вступає в дію 25 травня 2018 р.

Посібник може бути корисний працівникам органів та установ соціального захисту в Україні усіх рівнів, громадським активістам, якій працюють в сфері соціального захисту вразливих осіб та усім хто цікавиться захистом персональних даних в Україні.

Автори висловлюють вдячність Благодійному фонду «Стабілізейшнз суппорт сервісез» та Посольству Об'єднаного Королівства Великої Британії та Північної Ірландії в Україні за сприяння в підготовці та публікації цього посібника.

Список скорочень

Директива - Директива 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 року

ЄС – Європейський Союз

ЄСПЛ – Європейський суд з прав людини

Закон - Закон України «Про захист персональних даних» від 01 червня 2010 р. №2297-VI

Конвенція - Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28 січня 1981 р.

Регламент - Регламент Європейського Парламенту та Ради ЄС 2016/679 від 27 квітня 2016 р. «Про захист фізичних осіб щодо обробки персональних даних та вільного бігу таких даних», що замінює Директиву

РЄ – Рада Європи

Уповноважений – Уповноважений Верховної Ради України з прав людини

1. ДЖЕРЕЛА ПРАВОВОГО РЕГУЛЮВАННЯ ВІДНОСИН, ПОВ'ЯЗАНИХ З ОБРОБКОЮ ТА ЗАХИСТОМ ПЕРСОНАЛЬНИХ ДАНИХ.

1.1.Міжнародні документи.

Вперше своє нормативне закріплення норми з правового регулювання захисту персональних даних знайшли своє закріплення в положеннях міжнародних договорів з прав людини, як складова права на приватність. Так, у ст. 17 Міжнародного Пакту про громадянські та політичні права 1966 р. закріплено: «1. Ніхто не повинен зазнавати свавільного чи незаконного втручання в його особисте і сімейне життя, свавільних чи незаконних посягань на недоторканність його житла або таємницю його кореспонденції чи незаконних посягань на його честь і репутацію. 2. Кожна людина має право на захист закону від такого втручання чи таких посягань». Аналогічне за змістом положення включене і до ст. 16 Конвенції про права дитини 1989 р.

В подальшому в рамках Організації з економічного співробітництва та розвитку (далі – ОЕСР) було розроблено «Базові принципи захисту недоторканності приватного життя і транскордонних потоків персональних даних» (англ. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data), схвалені Рекомендацією Ради ОЕСР від 23 вересня 1980 р., нова редакція яких була ухвалена у 2013 р. Своєю чергою, Генеральна Асамблея ООН резолюцією №95 (XLV) прийняла «Керівні принципи регулювання комп'ютерних файлів, які містять персональні дані» (англ. Guidelines for the Regulation of Computerized Personal Data Files).

Крім універсальних міжнародних договорів, відповідні норми містилися і в регіональних міжнародних договорах щодо захисту прав людини. Так, положення щодо захисту права на приватність містяться в ст. 11 Американської конвенції з прав людини 1969 р., ст. 7 Хартії основних прав Європейського Союзу тощо

1.2.Рада Європи та Європейський Союз.

В ст. 8 Конвенції про захист прав людини і основоположних свобод 1950 р., зазначено: «Кожен має право на повагу до свого приватного і сімейного життя, до свого житла і кореспонденції». Заснований Конвенцією Європейський суд з прав людини (надалі – ЄСПЛ) у своєму рішенні у справі «Леандер проти Швеції» зазначив, що зберігання державними органами інформації про особу є втручанням у її право на повагу до – приватного життя, а відтак повинне відповідати вимогам, викладеним у частині 2 статті 8 Конвенції. В подальшому Європейський суд вказав, що держава повинна також вживати розумних заходів із метою дотримання права особи на повагу до її приватного життя (а відтак і права на захист персональних даних) з боку приватних суб'єктів. Перелік ключових рішень ЄСПЛ щодо захисту персональних даних та права на приватність містяться в Додатку №1.

28 січня 1981 року було прийнято Конвенцію № 108 Ради Європи «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних». У цьому документі було викладено ключові принципи обробки персональних даних, права особи у зв'язку з обробкою її персональних даних, базові норми щодо транскордонної передачі даних. У подальшому, а саме 8 листопада 2001 р., було прийнято Додатковий протокол до цього міжнародного договору, який деталізував положення Конвенції в частині, що стосується транскордонної передачі даних, та містив нові положення щодо необхідності створення Сторонами Конвенції наглядового органу, який би здійснював контроль за додержанням законодавства про захист персональних даних. Станом на сьогодні Комітетом Міністрів Ради Європи ведеться робота щодо оновлення вказаного документу.

Після прийняття Конвенції Комітетом міністрів Ради Європи велася активна робота в напрямку роз'яснення порядку застосування її положень в ході здійснення обробки, що несе найбільших ризик порушення прав людини. Із цією метою Комітет міністрів прийняв низку рекомендацій щодо обробки персональних даних у сферах соціального захисту,

страхування, охорони здоров'я, медицини та ін.[1]. Ці документи сприяють підтриманню положень Конвенції в актуальному стані.

Сьогодні локомотивом розвитку правового регулювання у сфері захисту персональних даних став Європейський Союз. Директива 95/46/ЄС Європейського Парламенту та Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 року (далі – Директива), яку з 25 травня 2018 року замінить Регламент про захист персональних даних, який набрав чинності 24 травня 2016 року (далі – «Регламент»), є, станом на сьогодні, передовими стандартами захисту персональних даних.

Попри те, що ці документи не є частиною національного законодавства, частина положень Директиви була включена в Закон України «Про захист персональних даних» (далі – «Закон»).

1.3.Національне законодавство.

На національному рівні ключовими документами у сфері захисту персональних даних є Конституція України, Закон України «Про захист персональних даних», документи у сфері захисту персональних даних, прийняті Уповноваженим Верховної Ради України з прав людини. Вагоме значення мають також низка інших законів, як наприклад, Закон України «Про доступ до публічної інформації» та Закон України «Про інформацію».

Відповідно до ст. 32 Конституції України ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків,

---

1 Зокрема, з останніх прийнятих рекомендацій Комітету Міністрів: Recommendation CM/Rec(2016)1 of the Committee of Ministers to member States on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality; Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment and Explanatory memorandum; Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a Guide to human rights for Internet users (Adopted by the Committee of Ministers on 16 April 2014 at the 1197th meeting of the Ministers' Deputies) та ін.

визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

Положення цієї статті було роз'яснено в рішенні 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 від 20 січня 2012 року. Крім цього, певний інтерес з точки зору захисту персональних даних становить рішення Конституційного Суду України у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України «Про інформацію» та статті 12 Закону України «Про прокуратуру» (справа К.Г. Устименка).

З метою імплементації Конвенції Верховною Радою України 1 червня 2010 р. було прийнято Закон, який закріплює основні принципи обробки персональних даних, права суб'єктів персональних даних, основні підстави обробки персональних даних, принципи обмеження дії Закону, повноваження наглядового органу та ін. На виконання Закону наглядовим органом у сфері захисту персональних даних, яким є станом на сьогодні Уповноважений Верховної Ради України з прав людини, наказом від 8 січня 2014 року № 1/02-14 було затверджено низку підзаконних актів у сфері захисту персональних даних:

Типовий порядок обробки персональних даних - даний документ містить ключові зобов'язання володільців щодо організації процесу обробки персональних даних.

Порядок здійснення Уповноваженим ВРУ контролю за додержанням законодавства про захист персональних даних – даний документ регламентує порядок проведення перевірки володільців Уповноваженим Верховної Ради України з прав людини;

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

2. ВИЗНАЧЕННЯ КЛЮЧОВИХ ТЕРМІНІВ

2.1. Персональні дані. Визначення та розуміння поняття «персональні дані» є однією із найважливіших при роботі в цій сфері. У Регламенті, Директиві, Конвенції та Законі поняття персональних даних визначено приблизно однаково, а саме як: «будь-яка інформація, яка стосується ідентифікованої особи або особи, яка може бути ідентифікованою».

Ключовим у вищенаведеному визначенні також є поняття «ідентифікована особа». Таким чином, ідентифікованою є особа, яку за наявною в розпорядженні володільця інформацією можна безпомилково виділити з-посеред інших осіб. Зазвичай для того, щоб вважати особу ідентифікованою, необхідні її ім'я, прізвище, по батькові та реквізити документа, що посвідчує особу/цифровий номер, що присвоюється особі (наприклад, ідентифікаційний номер фізичної особи). Однак, за певних умов наявність меншої кількості інформації чи певного об'єму іншої інформації є достатніми для того, щоб ідентифікувати особу (див. приклади нижче). Більше деталей у цьому відношенні передбачає Регламент.

Приклад 1. В під'їзді багатоповерхового житлового будинку розвішується інформація щодо осіб, які заборгували гроші за комунальні послуги, з вказівкою номеру квартири та суми заборгованості. Для сусідів суб'єкта вказаної інформації достатньо для того, щоб його ідентифікувати.

Приклад 2. В районному відділі соціального захисту розвішується інформація щодо надання конкретним жителям району соціальних послуг та соціального обслуговування із вказівкою прізвища, ініціалів особи та виду наданої послуги. Такої інформації в багатьох випадках буде достатньо для того, щоб провести ідентифікацію особи.

Приклад 3. Компанія, що володіє медичними даними пацієнтів, розділяє дані щодо стану здоров'я та особисті дані особи, що дають змогу її ідентифікувати. При цьому, використовується шифр, який присвоюється вказаним групам даних, та в разі потреби надасть можливість встановити, кому із пацієнтів належать медичні дані. Знеособлені таким чином відомості щодо стану здоров'я передаються іншій компанії для проведення наукових досліджень. В цьому випадку, провести ідентифікацію буде практично неможливо, через заходи із знеособлення.

Регламент містить найбільш сучасне та практичне визначення «особи, що може бути ідентифікованою», згідно з яким це «особа, яку можна ідентифікувати прямо чи опосередковано, зокрема вказавши такі ідентифікатори, як ім'я, ідентифікаційний номер, дані щодо місцезнаходження, он-лайн ідентифікатор чи інші особливості фізичної, фізіологічної, генетичної, духовної, економічної, культурної чи соціальної ідентичності такої фізичної особи».

Щодо класифікації **видів персональних даних**, слід зазначити, що такими актами, як Закон (ст. 7), так і Директива (ст. 8), Регламент (ст. 9) та Конвенція (ст. 6), із загального переліку персональних даних виділяються спеціальні, чутливі категорії персональних, обробка яких дозволяється лише у чітко визначених випадках.

До таких категорій вказані правові акти відносять персональні дані про: расове або етнічне походження; політичні, релігійні або світоглядні переконання; членство в політичних партіях та професійних спілках; засудження до кримінального покарання; дані, що стосуються здоров'я, статевого життя, а також біометричні або генетичні дані.

Обробка цих категорій персональних даних здійснюється в спеціальному порядку, який регламентується окремо.

2.2.Обробка персональних даних. Відповідно до Закону, обробка персональних даних – це «будь-яка дія або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання

і поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем».

Всупереч поширеному помилковому твердженню обробкою є не лише вчинення вказаних дій із систематизованою сукупністю персональних даних великої кількості осіб (базою даних, реєстром, каталогом, досьє тощо). Просте зберігання володільцем, навіть у недоступному вигляді, інформації про хоча б одного суб'єкта персональних даних є обробкою відповідно до положень Закону. Таким чином, наявність будь-якого документу, що містить персональні дані особи, на робочому столі чи в сейфі державного службовця становитиме обробку персональних даних цієї особи.

Разом з тим, слід зазначити, що **не всі види обробки персональних даних потрапляють в сферу дії Закону**.

Так, згідно з частиною 2 статті 25 Закону його положення не застосовується до:

- обробки персональних даних у приватних цілях;
- обробки персональних даних у журналістських цілях;
- обробки персональних даних у творчих цілях;
- відносини щодо отримання архівної інформації репресивних органів.

Обробка персональних даних у приватних цілях. Так, ведення особою телефонної книги належить до приватних цілей. Однак, якщо ця особа є власником бізнесу (наприклад, ресторанів чи магазинів) і збирає персональні дані клієнтів (ім'я, прізвище, по батькові і номер телефону/адреса проживання) для використання в комерційних цілях, як то реклама та просування власних послуг, то це вже не може вважатися обробкою у приватних цілях, незважаючи на те, що здійснюється окремою особою для потреб власного бізнесу.

На ***обробку персональних даних у журналістських та творчих цілях*** положення Закону не поширюються **за умови забезпечення балансу між правом на повагу до особистого життя та правом на свободу вираження поглядів**. За звичайних умов специфіка журналістської діяльності не потрапляє в сферу дії Закону. Однак якщо втручання в право

особи на повагу до приватного життя внаслідок обробки її персональних даних журналістами є надмірним у порівнянні з суспільним інтересом до висвітленої інформації (персональних даних особи) чи її суспільною вагою, можуть підніматися питання додержання законодавства про захист персональних даних.

Приклад. На веб-сайті одного із засобів масової інформації було викладено інформацію щодо осіб, які не з'явилися до військового комісаріату після вручення їм повістки. Висвітлення такої інформації є очевидним порушенням балансу між суспільними інтересами та правом окремої особи на захист її приватності. Дійсно ухилення від військової служби у той час як держава перебуває в стані збройного конфлікту є актуальною темою. Однак, оприлюднення персональних даних вказаних осіб жодним чином не сприяло висвітленню цієї тематики, достатньо було навести звичайну статистичну інформацію. Натомість абсолютно очевидно, що адміністрація сайту переслідувала мету стигматизації цих осіб як таких, що в тяжкий для держави час ухиляються від виконання свого військового обов'язку. Відтак, така обробка персональних даних повинна відповідати положенням Закону, що за даних обставин (відсутність легітимної мети та законних підстав поширення персональних даних призовників) майже автоматично становитиме його порушення.

Щодо *архівної інформації репресивних органів*, то обробка такої інформації, в силу її специфіки, окремо регламентується Законом України «Про доступ до архівів репресивних органів комуністичного тоталітарного режиму 1917 - 1991 років».

2.3.Знеособлення персональних даних. Під знеособленням розуміється вилучення відомостей, які дають змогу прямо чи опосередковано ідентифікувати особу. Вказане положення необов'язково передбачає повне видалення будь-яких даних, що дають можливість ідентифікувати суб'єкта (хоч така операція і охоплюється терміном знеособлення).

Натомість мова йде скоріше про вжиття заходів, спрямованих на унеможливлення ідентифікації суб'єктів володільцем, у чиєму розпорядженні перебувають їх персональні дані/ працівниками, що використовують ці дані.

Приклад. Лікарня створює реєстр пацієнтів, де обробляються виключно особисті дані (ім'я, прізвище, по батькові, адреса, телефон). Цим даним присвоюється певний ідентифікатор. З медичних документів кожного із внесених до реєстру пацієнтів видаляються (ретушуються) особисті дані та проставляється ідентифікатор, після чого документи відправляються в архів. Таким чином, лише той, хто має доступ до реєстру знатиме, кому належить документація. Той, хто працюватиме з медичними документами (науковець, студент, службовець управління охорони здоров'я) не зможе ідентифікувати особу, оскільки працюватиме із знеособленими даними.

2.4.Володілець персональних даних. Згідно з визначенням, викладеним у Законі, володілець персональних даних – це фізична або юридична особа, яка визначає мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом (ст. 2).

Виходячи з його положень, не викликає труднощів визначення володільця, коли мова йде **про приватних суб'єктів**, які в більшості випадків дійсно самостійно визначають ціль обробки, склад даних та процедури їх обробки. Дещо інша ситуація, коли мова йде про обробку персональних даних, наприклад ведення реєстру, **державними органами влади**. У таких випадках мета обробки, склад даних, порядок їх обробки, як і те, хто є володільцем, зазвичай визначено законодавством, а не самим володільцем. Слід наголосити, що на практиці саме **законодавством** визначається володілець, а не **законом**, як це вказано у визначенні.

Приклад 1.
Згідно з Законом України «Про збір та облік єдиного внеску на загальнообов'язкове державне соціальне страхування» Реєстр застрахованих осіб «формує та веде Пенсійний фонд».
Відтак **Пенсійний фонд України і буде володільцем** даного реєстру.

Приклад 2.
Згідно з Положенням про електронний реєстр пацієнтів, затвердженим постановою КМУ від 6 червня 2012 року № 546 «Розпорядником реєстру є МОЗ. (…) 9. Володільцями реєстру є заклади охорони здоров'я.»

Разом з тим, слід зазначити, що інколи положення законодавства настільки заплутані з точки зору понятійного апарату, що визначення того, хто є володільцем, доводиться здійснювати самостійно, виходячи з фактичних обставин.

Приклад
Згідно з Порядком ведення реєстру хворих на туберкульоз, затвердженим наказом МОЗ № 818 від 19.10.2012 року:
«- **адміністратор другого рівня** - посадова особа, яка здійснює контроль за наповненням реєстру баз персональних даних хворих на туберкульоз у межах компетенції відповідного органу державної влади, підприємства, установи, організації, певного регіону, моніторинг роботи реєстру баз персональних даних хворих на туберкульоз (далі - Реєстр) та коригування структури відомостей про хворих на туберкульоз (далі - Відомості).

- **адміністратор Реєстру** - центральний орган виконавчої влади у сфері охорони здоров'я або його структурний підрозділ, що здійснює заходи зі створення та супроводу програмного забезпечення Реєстру, збереження та захисту бази даних Реєстру, відповідає за його функціонування та надає доступ до нього;
- база персональних даних - іменована сукупність упорядкованих персональних даних хворих на туберкульоз в електронній формі;
- **володільці баз персональних даних** - Протитуберкульозні заклади;
- **користувачі** - працівники Протитуберкульозних закладів, які визначені відповідними наказами Протитуберкульозних закладів відповідальними особами за ведення Реєстру та нерозголошення Відомостей, які стали їм відомі при роботі з Реєстром;
- **реєстр баз персональних даних хворих на туберкульоз** - інформаційна система збору, накопичення, обробки, оновлення, використання та поширення Відомостей, що складається з баз персональних даних;
- **розпорядник бази персональних даних** - Міністерство охорони здоров'я України.»

З огляду на вказані положення протитуберкульозні заклади є спів-володільцями реєстру. При цьому не зрозуміло, чи мають вони доступ до всіх баз персональних даних «реєстру баз персональних даних хворих на туберкульоз» чи лише до бази даних власних пацієнтів. Повноваження «**розпорядника бази персональних дани**х» взагалі незрозумілі, оскільки поняття «розпорядник» зустрічається лише у визначенні. Повноваження інших роботи із реєстром / базою персональних даних / реєстром баз персональних даних також недостатньо визначені. Відтак, володільця можливо визначити лише ознайомившись із фактичною організацією роботи реєстру.

Очевидно, що законодавство України потребує

подальшого вдосконалення в частині підбору понятійного апарату.

Інколи законодавство не визначає, хто є володільцем, відтак, як і у вказаному вище випадку володільця необхідно визначати, виходячи з фактичної ситуації.

Окрім того, слід зазначити, що в залежності від того скільки є володільців бази даних і які у них повноваження можна виділити декілька окремих ситуацій:

- якщо одні і ті ж дані окремо зберігаються у декількох суб'єктів (наприклад юридичних осіб), вони усі є незалежними один від одного володільцями;

- якщо рівним доступом до однієї бази даних користуються два суб'єкти і кожен може приймати на свій розсуд рішення (будь-які рішення чи в межах своїх повноважень) щодо обробки наявних у ній даних, їх слід розглядати як співволодільців;

Приклад

Згідно з пунктом 6 постанови КМУ № 121 від 16 лютого 2011 року «Про затвердження Положення про централізований банк даних з проблем інвалідності» «операторами банку даних є:

1) центрального рівня – Мінсоцполітики, МОЗ, МОН, МВС, Мінмолодьспорт, та Державна служба у справах ветеранів війни та учасників антитерористної операції;

2) місцевого рівня: орган виконавчої влади в Автономній Республіці Крим з питань соціального захисту населення, структурні підрозділи з питань соціального захисту населення обласних, Київської та Севастопольської міських держадміністрацій; структурні підрозділи з питань соціального захисту населення районних, районних у мм. Києві та Севастополі держадміністрацій, виконавчих органів міських, районних у містах (крім мм. Києва та Севастополя) рад (…).

Одночасно декілька з вказаних органів мають певні повноваження щодо внесення та перегляду інформації в реєстрі. Відтак, вони усі є спів-володільцями вказаної бази даних.

- якщо двоє чи більше суб'єктів мають різні рівні доступу до однієї бази даних і кожен може приймати рішення щодо обробки наявних у ній даних, до яких він має доступ, кожен з них є володільцем даних, до яких лише він має доступ та спів володільцем даних, щодо яких інший володілець також має повноваження щодо обробки.

Слід зазначити, що поняття «спів-володілець» відсутнє в українському законодавстві, однак логічно випливає із вказаних вище ситуацій. Як Директива, так і Регламент включають поняття спів-володільця. Так, згідно з Регламентом, «володілець – фізична чи юридична особа, орган влади, державне агентство чи інша установа, яка самостійно чи спільно з іншими, визначає мету та спосіб обробки даних».

2.5.Розпорядник персональних даних. Відповідно до ст. 2 Закону, розпорядником персональних даних є «фізична чи юридична особа, якій володільцем персональних даних або законом надано право обробляти ці дані від імені володільця». Відповідно до ст. 4 Закону, **розпорядником персональних даних, володільцем яких є орган державної влади чи орган місцевого самоврядування, крім цих органів, може бути лише підприємство державної або комунальної форми власності**, що належить до сфери управління цього органу. Володілець персональних даних може доручити обробку персональних даних розпоряднику персональних даних відповідно до договору, укладеного в письмовій формі. Розпорядник персональних даних може обробляти персональні дані лише з метою і в обсязі, визначених у договорі.

Приклад.

Підприємства, що надають житлово-комунальні послуги, укладають договори з приватними компаніями, на підставі яких останні ведуть облік кількості та якості послуг, наданих підприємством споживачам, та облік здійснення споживачами оплати за вказані послуги. У вказаному договорі підприємства визначають мету обробки, склад даних, повноваження компаній щодо обробки персональних даних споживачів, зобов'язання щодо їх захисту та відповідальність за порушення договору. Таким чином, компанії обробляють персональні дані споживачів за вказівкою підприємства та у визначених ним межах. Фактично такі компанії забезпечують технічну сторону функціонування реєстру. Відтак, такі компанії є розпорядниками.

2.6.Треті особи, одержувач та Уповноважений ВРУ з прав людини. Відповідно до Закону одержувач персональних даних – це «фізична чи юридична особа, якій надаються персональні дані, у тому числі третя особа»; третя особа – це будь-яка особа, за винятком суб'єкта персональних даних, володільця чи розпорядника персональних даних та Уповноваженого ВРУ з прав людини, якій володільцем чи розпорядником персональних даних здійснюється передача персональних даних».

Як видно із вказаних, визначень поняття одержувача є ширшим та включає поняття третьої особи. Ключова відмінність у тому, що третя особа є окремим від володільця персональних даних суб'єктом. Передача персональних даних третій особі потребує наявності однієї з правових підстав, передбачених статтею 11 Закону (див. нижче). Одержувачем можуть бути як треті особи, так і, наприклад, працівники володільця, структурні підрозділи, яким володілець може надати право доступу до персональних даних, які ним обробляються.

Однак, за певних умов і передача персональних даних одним працівником володільця іншому може розглядатися як передача (поширення) персональних даних третій особі.

Наприклад, якщо володільцем чітко розмежовано серед його працівників рівні доступу до персональних даних в базі даних і працівник, що має такий доступ, передає персональні дані працівнику, який такого доступу не має, така дія розглядатиметься як передача персональних даних третій особі. При цьому така дія буде скоріш за все незаконною.

Відповідно до частини першої ст. 4 Закону до складу суб'єктів, пов'язаних із відносинами щодо персональних даних, належить також Уповноважений ВРУ з прав людини, як орган, що здійснює контроль за додержанням законодавства про захист персональних даних. Детальніше про Уповноваженого Верховної Ради України з прав людини та його повноваження у цій сфері мова йтиме нижче.

3. ПРИНЦИПИ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

3.1. Загальна частина. Обробка персональних даних ґрунтується на низці принципів, які визначають основні правові засади її здійснення. Вказані принципи викладено у статті 5 Конвенції, статті 6 Директиви, статті 5 Регламенту та статті 6 Закону. Фактично під принципами розуміються правила, що повинні дотримуватися (за незначними виключеннями, про які йтиметься нижче) будь-яким володільцем в ході здійснення будь-якої обробки, на яку поширюються вказані документи. В узагальненому вигляді вказані принципи можна викласти наступним чином:

- законності та справедливості (англ. fairness, станом на сьогодні цеq принцип частіше формулюється як *принцип прозорості обробки персональних даних*);
- легітимної мети;
- пропорційності персональних даних щодо легітимної мети;
- точності (достовірності), актуальності персональних даних;
- обробка персональних даних у формі, що допускає ідентифікацію фізичної особи, якої вони стосуються, не довше, ніж це необхідно для законних цілей, у яких

вони збиралися або надалі оброблялися.

Інколи до вказаних принципів додається також принцип ***підзвітності***, що вперше з'являється в ч. 2 ст. 5 Регламенту. Згідно з даним принципом кожен володілець повинен бути здатним в будь-який продемонструвати дотримання вказаних принципів на практиці.

Також ч. 1 ст. 5 Регламенту передбачено принцип, відповідно до якого персональні дані повинні оброблятися у спосіб, що забезпечує достатній рівень їх захисту.

Інші положень вищезазначених актів є логічним продовженням, розвитком, деталізацією вказаних принципів і повинні тлумачитися у їх світлі. Наприклад, положення щодо інформування суб'єкта про обробку персональних даних (ст. 12 Закону), його права отримувати інформацію про те, чи обробляються його персональні дані, ким обробляються, який порядок обробки (стаття 8 Закону) є деталізацією принципу справедливості обробки. Право суб'єкта вносити зміни до змісту персональних даних, що обробляються володільцем, зокрема в разі їх неактуальності (стаття 8 Закону), та порядок його реалізації є, своєю чергою, втіленням принципу точності та актуальності. Положення щодо підстав обробки (стаття 11 Закону, стаття 5 Конвенції та стаття 6 Директиви) є втіленням розширеним викладом принципу законності і т. д.

3.2. Законність обробки персональних даних. Вказаний принцип, який закріплено в п. а. ч. 1 ст. 5 Конвенції, п. а. ч. 1 ст. 6 Директиви, ч. 1 ст. 6 Регламенту, а також ст. 6 Закону.

Більш детально він розкривається у практиці ЄСПЛ. Так, згідно з статтею 8 Конвенції втручання в гарантовані нею права (йдеться про право на повагу до приватності, яке серед іншого, включає право на захист персональних даних) можливо лише за умови його здійснення «згідно із законом». Поняття «згідно із законом» не лише вимагає, щоб відповідні заходи мали певну підставу в «законі», але й ставить вимогу щодо якості такого «закону», вимагаючи щоб він був **доступним** особі, якої стосується, та **передбачуваним** в частині наслідків його застосування. Вимога щодо доступності зазвичай

виконується якщо той чи інший нормативно-правовий акт було оприлюднено. Щодо вимоги передбачуваності то Суд встановив, що норма є «передбачуваною», якщо вона **сформульована з чіткістю, достатньою для того, щоб особа мала змогу, користуючись в разі потреби відповідною допомогою, регулювати свою поведінку** (див. рішення у справі «Ротару проти Румунії», заява № 27798/95, п. 48 – 49).

Відтак, для того, щоб бути законною, обробка персональних даних повинна:

1) базуватися на положеннях законодавства (більш детально про законодавчі підстави обробки див. розділ 3)**;**

2) таке законодавство повинне відповідати критеріям передбачуваності (більш детально про вказану вимогу див. частину … розділу 5)**.**

Класичним прикладом у цьому відношенні є рішення ЄСПЛ у справі «Ротару проти Румунії».

Приклад.
У справі "Rotaru v. Romania"[2] Служба розвідки Румунії (далі – СР) володіла файлом, що містив персональні дані заявника (інформація про навчання, громадську активність, публікації, участь в політичних організаціях та ін.). Заявник стверджував, що зберігання вказаної інформації СР було незаконним. Суд вказав, що єдиною підставою для такого накопичення була норма в законі про СР, згідно з якою СР мала право збирати, зберігати та використовувати інформацію, що має значення для національної безпеки. Суд зазначив, що жоден закон не визначав межі реалізації вказаних повноважень. Законодавство не передбачало, *яка інформація може зберігатися, категорії осіб, щодо яких вона може збиратися, обставини, за настання яких, може здійснюватися такий збір інформації, процедура збору, строки зберігання такої інформації, хто має доступ до файлів, як вони можуть використовуватися та який характер цих файлів*. Суд також зазначив, що зберігання та використання такої інформації не супроводжувалося відповідними гарантіями від зловживань, зокрема *не було незалежного контролю* (наприклад, судового) за діяльністю СР в цій частині. З огляду на зазначені факти Суд вказав, що законодавство, що регламентувало втручання в права заявника (обробка СР його персональних даних) не було достатньо передбачуваним. Відтак, втручання в його права не було *законним* і порушувало статтю 8 Конвенції.

3.3. Визначеність мети. Згідно з ч. 1 ст. 6 Закону мета обробки персональних даних має бути сформульована в законах, інших нормативно-правових актах, положеннях, установчих чи інших документах, які регулюють діяльність володільця персональних даних, та відповідати законодавству про захист персональних даних. Вказане положення закону є результатом імплементації п. b) ч. 1 ст. 5 Конвенції («Якість даних»), відповідно до якого персональні дані, що піддаються автоматизованій обробці повинні зберігатися для **чітких**

2 Rotaru v. Romania [GC], no. 28341/95, ECHR 2000 V

та **легітимних** цілей і не використовуватися у спосіб, що суперечить цим цілям.

Чіткість формулювання є основним кроком гарантування законності обробки. Так, будь-яка дія, яка здійснюється щодо персональних даних повинна відповідати визначеній меті їх обробки. Відтак, саме мета закладає базові межі обробки, необхідні для того, щоб надати суб'єкту персональних даних картину того, як оброблятимуться дані, а відтак і можливість контролювати їх обробку.

Приклад.

Згідно з пунктом 1 Положення про централізований банк даних з проблем інвалідності**,** визначено порядок створення, функціонування та ведення централізованого банку даних з проблем інвалідності як автоматизованої системи для визначення потреб осіб з інвалідністю та дітей з інвалідністю у засобах і послугах реабілітації.

Відтак, дане положення чітко визначає мету обробки даних.

Разом з тим, згідно з пунктом 8 Положення до повноважень операторів банку даних місцевого рівня належить: (…) ведення обліку бездомних громадян (…).

З огляду на формулювання мети (*визначення потреб осіб з інвалідністю та дітей з інвалідністю у засобах і послугах реабілітації*) незрозуміло до чого тут *бездомні громадяни*. Обробка даних таких громадян у вказаному реєстрі буде незаконною, оскільки не відповідає поставленій меті функціонування реєстру.

Звідси випливає і те, що мета не може бути викладеною таким чином, щоб надати необмежені чи невизначені можливості щодо обробки персональних даних. Більше того, навіть якщо суб'єкт персональних даних або закон дозволяє вчиняти з персональними даними дії, які не є необхідними для досягнення задекларованої мети, такі дії будуть незаконними та потребуватимуть внесення змін до закону чи модифікації умов згоди.

Персональні дані, зібрані для різних цілей не повинні об'єднуватися, крім випадків, коли вказані цілі є сумісними, а склад персональних даних, які необхідні для досягнення обох цілей, збігається.

Метою обробки персональних даних не може бути сам факт обробки. Часто трапляються ситуації, коли в якості мети вказується «необхідність ведення обліку», «накопичення якомога більшої кількості інформації» та ін. В такому випадку складається ситуація, коли облік (який і є нічим іншим як обробкою персональних даних) ведеться заради обліку (див. Приклад).

Приклад.
У справі «M.K. v. France»[3] заявника було затримано за крадіжку та відібрано відбитки пальців. В подальшому справу було закрито. Заявник звернувся до прокурора з вимогою видалити відбитки пальців, однак йому було відмовлено. Суди залишили без змін рішення прокурора з огляду на необхідність *накопичення якомога більшої кількості зразків для порівняння* для полегшення розслідувань. Суд вказав, що цілі обробки відбитків пальців у вказаній базі даних, вказані судами були настільки широкими, що фактично санкціонували зібрання відбитків всього населення, що було очевидно непропорційним. Таким чином, держава, на думку Суду, вийшла за межі наданої їй свободи розсуду і не збалансувала інтересів особи з суспільними та порушила статтю 8 Конвенції.

Згідно з ч. 1 ст. 6 Закону у разі зміни визначеної мети обробки персональних даних на нову мету, яка є **несумісною** з попередньою, для подальшої обробки даних володілець персональних даних повинен отримати згоду суб'єкта персональних даних на обробку його даних відповідно до зміненої мети, якщо інше не передбачено законом.

Якщо аналізувати вказані положення Закону з

3 M.K. v. France, no. 19522/09, 18 April 2013

урахуванням міжнародних документів, про які мова йшла вище, то видається логічним, що як ***сумісні*** в сенсі ч. 1 ст. 6 Закону слід розглядати наукові, історичні та статистичні цілі. **Відтак, подальша обробка зібраних до того персональних даних в історичних, статистичних чи наукових цілях не потребує наявності окремої підстави**. Однак, це можливо за умови «забезпечення їх належного захисту» (ч. 8 ст. 8 Закону)/ за умови «наявності достатніх гарантій» (ст. 6 Директиви, Рекомендації РЄ[4]).

3.4. Адекватність, відповідність та ненадмірність. Відповідно до вказаного принципу склад та зміст персональних даних, що обробляються володільцем повинні відповідати легітимній меті їх обробки, бути відповідними, адекватними та ненадмірними щодо такої мети. Тобто, **по-перше**, оброблятися повинні виключно ті дані, обробка яких необхідна для досягнення мети (див. Приклад 1), і, **по-друге**, навіть якщо певні дані і використовуються для досягнення мети, їх обробка буде незаконною, якщо її можна досягти і не здійснюючи обробки вказаних даних (див. Приклад 2). Більш того, принцип пропорційності повинен охоплювати увесь процес будь-якої обробки персональних даних. Так, як зазначалося вище, обробка персональних даних повинна здійснюватися не довше, ніж це необхідно для законних цілей, у яких вони збиралися або надалі оброблялися. Також рівень організаційно-технічного захисту персональних даних повинен бути пропорційним характеру та об'єму персональних даних, що обробляються.

4 Рекомендація КМ РЄ № R (97) 5 щодо захисту персональних даних, які збираються та обробляються в цілях статистики; Рекомендація КМ РЄ № R (97) 18 щодо захисту медичних даних.

Приклад 1.
Справа «L.H. v. LATVIA»[5].
У 1997 році заявниці довелося терміново робити кесарів розтин. В ході операції хірург без згоди на то заявниці провів стерилізацію. Інспекція, що здійснювала контроль за якістю надання медичної допомоги, провела перевірку щодо даного інциденту. З цією метою нею було зібрано відомості щодо надання заявниці медичної допомоги з 1996 по 2003 роки.
Заявниця оскаржила факт збору чутливої інформації щодо неї Інспекцією, однак судами було відмовлено в задоволенні її позову.
Досліджуючи питання необхідності збору інформації щодо заявниці Суд, серед іншого, звернув увагу на те, що Інспекцією було зібрано непропорційно великий об'єм інформації (за період тривалістю сім років (за рік до операції та 6 після) з 3-ох установ), щоб оцінити одне хірургічне втручання у 1997 році. Цьому не було надано жодного обґрунтування. Відтак, Суд констатував непропорційність втручання в права заявниці, гарантовані статтею 8 Конвенції.

Приклад 2.
МОЗ через Департамент охорони здоров'я ОДА (далі - Департамент) звернувся до лікарні з вимогою направити копії обмінних карт вагітних з результатами дополологових обстежень в усіх випадках народження дітей із синдромом Дауна. Вказані документи було направлено. Згідно із запитом вказані документи запитувалися з метою проведення дослідження, необхідного для удосконалення пренатальної діагностики медичними закладами. В подальшому їх було направлено вказаному досліднику.
Вказане наукове дослідження повинне було проводитися дослідником, тому, направлення копій документів, що містять чутливу інформацію про стан здоров'я, Департаменту / МОЗ, а не безпосередньо досліднику, не було необхідним заходом.

5 L.H. v. Latvia, no. 52019/07, 29 April 2014

Вказаний принцип повинен пронизувати **будь-який процес обробки персональних даних незалежно від підстав її здійснення**.

Навіть, якщо особа надала згоду на обробку її персональних даних, які по своїй суті не є необхідними для досягнення мети обробки, така обробка суперечитиме Закону.

Крім цього, проведення вказаного дослідження очевидно не потребувало використання особистих даних пацієнтів (імені, прізвища та по батькові). Для проведення дослідження необхідною була сласне медична інформація. Крім цього, від лікарні було отримано відносно невелику кількість копій обмінних карт. Тому знеособлення вказаних документів не становило би надмірного тягаря для медичного закладу. Однак, цього зроблено не було. Такі дії лікарні також становили порушення вказаного положення Закону.

У зв'язку з цим неприйнятними є ситуації, коли в особи береться **«необмежена згода на обробку персональних даних»** та **«безвідклична згода»**. Чітко сформульована мета повинна надати можливість володільцю з високим ступенем ймовірності передбачити об'єм персональних даних, необхідних для її досягнення.

Якщо обробка персональних даних здійснюється з метою виконання повноважень державного органу (більш детально про законні підстави обробки див. розділ 3), оброблятися повинні лише ті персональні дані, які необхідні для належного виконання цих повноважень. З огляду на те, що обробка в таких випадках здійснюється на підставі закону та в порядку визначеному законодавством, саме нормативно-правовими актами повинен визначатися склад даних, який би був пропорційним меті їх обробки. Тому пропорційність обробки повинна закладатися в нормативно-правовий акт вже на етапі проекту. Роз'яснення того, чому проектом нормативно-правового акту, передбачається певний склад персональних

даних, що оброблятиметься повинно бути викладено в супровідній пояснювальній документації до законопроекту. Оскільки не завжди можливо передбачити оптимальний склад даних, що необхідні для виконання повноважень державного органу законодавство повинно надавати певну дискрецію державному органу, **щоб враховувати індивідуальну ситуацію суб'єкта персональних даних. Наприклад, щоб в разі надходження звернення від такого суб'єкта щодо припинення обробки, зміни чи виправлення його персональних даних, мати можливість вжити відповідних заходів.**

Приклад. Справа «Гардель проти Франції»[6].
У Франції було прийнято закон про створення Єдиного реєстру осіб, що вчинили статеві злочини. Персональні дані заявника після вчинення ним зґвалтування було внесено до вказаного реєстру. Заявник стверджував, що зберігання його персональних даних у вказаному реєстрі було непропорційним заходом. Суд наголосив, що ведення реєстру було *необхідним та пропорційним у світлі вказаної мети* та супроводжувалося відповідними гарантіями захисту від порушення прав суб'єктів, оскільки, окрім іншого, в разі необхідності 1) строк зберігання інформації у реєстрі міг бути переглянутий в будь-який час до його завершення (з огляду на вік особи, плин часу, зміну особистості, життєвих обставин та ін.), а 2) рішення про відмову в перегляді могло бути оскаржено до суду.

Якщо обробка здійснюється з метою виконання обов'язку, передбаченого законом (наприклад, надання у випадках та в порядку, визначених законодавством, інформації за запитами правоохоронних та податкових органів та ін.), володільці повинні враховувати, які дані необхідні для його виконання. При цьому і той, хто запитує персональні дані, повинен враховувати принцип необхідності та запитувати лише ті дані, що необхідні для досягнення визначеної мети.

6 Gardel v. France, no. 16428/05, ECHR 2009

Якщо ж склад таких даних визначено законодавством, як це часто трапляється, саме воно повинно, як і у випадку вище, враховувати дотримання принципу необхідності.

3.5. Достовірність та точність. Персональні дані, що обробляються володільцем повинні бути точними та достовірними. Це зобов'язання володільця передбачає, що з його сторони вживатимуться розумні заходи спрямовані на те, щоб підтримувати персональні дані суб'єкта в актуальному стані, а суб'єкту персональних даних забезпечується право звертатися до володільця з вимогою виправити його персональні дані.

При цьому допускаються певні відступи від вказаного принципу в залежності від того, про яку сферу діяльності йде мова (медична інформація, інформації щодо причетності особи до вчинення того чи іншого злочину та ін.).

3.6. Справедливість обробки персональних даних (англ. fair processing). Вказаний принци закріплено як у Конвенції (п. (а) ст. 5), Директиві (ст. 6), Регламенті (ст. 5), так і у Законі. Згідно з п. 2 ч. 1 ст. 6 Закону «обробка персональних даних здійснюється **відкрито і прозоро** із застосуванням засобів та у спосіб, що відповідають визначеним цілям такої обробки».

В загальних рисах вказаний принцип передбачає, що інформація щодо здійснення володільцем обробки персональних даних повинна бути відкритою, регламентуватися зрозумілими та доступними правилами, а суб'єкт персональних даних повинен знати про обробку його персональних даних, про те, які дані обробляються, та мати певні можливості щодо контролю обробки.

Попри різні формулювання розуміння вказаного принципу є здебільшого однаковим та включає в себе такі права та обов'язки суб'єктів та володільців:

1) інформування суб'єкта персональних даних щодо обробки його персональних даних. Вказане зобов'язання передбачає обов'язок володільця автоматично надавати суб'єкту певну інформацію про обробку його персональних даних. Дане

правило деталізується в пп. 1, 2 ч. 2 ст. 8 та ч. 2 ст. 12 (див. також ст. 10 – 11 Директиви, ст. 13 – 14 Регламенту; в Конвенції окремої статті, присвяченої цьому питанню немає, однак воно включено в проект модернізованої Конвенції (стаття 7bis)[7]. Вказані положення деталізують об'єм інформації, що надається, та момент її надання.

2) право доступу суб'єкта персональних даних, згідно з яким він має право знати, ким та яким чином обробляються його персональні дані, а також їх склад та зміст. Із вказаного правила випливає право суб'єкта на виправлення, видалення та блокування його персональних даних в разі порушення якогось із зазначених вище принципів (ст. 8 Конвенції, ст. 12 Директиви, ст. 15 – 16 Регламенту, пп. 3, 4, 5 та 6 ч. 2 ст. 8, ч. 6 ст. 16, ст. 20 та 21 Закону).
3) право суб'єкта направляти заперечення проти обробки його персональних даних з посиланням на вагомі та легітимні особисті обставини, право суб'єкта заперечити проти автоматизованого індивідуального рішення щодо нього та проти обробки персональних даних з метою здійснення цільового маркетингу. Вказані права чітко викладено в Директиві (стаття 15) та Регламенту (ст. 21 – 22), однак в Конвенції відсутні. У Законі вказані права викладено в загальних рисах у пп. 5, 12 та 13 ч. 2 ст. 8;
4) повідомлення наглядового органу у визначених законом випадках про обробку персональних даних та оприлюднення останнім такої інформації.

З огляду на те, що кожне з вказаних питань потребує додаткових роз'яснень, вони будуть розглянуті в окремому розділі нижче.

3.7. Принцип підзвітності, хоч і окремо не передбачено національним законодавством, імпліцитно випливає із норм Закону, якщо розглядати їх у світлі вказаних міжнародних документів.

---

7 Report of the 3rd CAHDATA meeting, CM(2015)40 http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/CAHDATA%203_Report_CM(2015)40_En.pdf

Так, передбачене Законом (п. 8 ч. 2 ст. 8 та ст. 23) право застосовувати засоби правового захисту та звертатися зі скаргою передбачає не лише гарантії незалежного та безстороннього розгляду скарги та прийняття рішення, здатного виправити порушення прав суб'єкта в разі якщо воно мало місце, а й повинно гарантувати наявність в контролюючого органу (Уповноваженого ВРУ з прав людини) чи суду можливість належним чином перевірити дотримання володільцем законодавства про захист персональних даних. Це було б неможливо, якби володілець міг не зберігати інформацію щодо обробки персональних даних (чи безслідно знищити її) та в разі отримання скарги посилатися на неможливість доведення його причетності/вини в порушенні законодавства про захист персональних даних. Саме володілець повинен в разі направлення суб'єктом скарги надати докази того, що ним не було вчинено порушення.

Вказане підтверджується також правом особи отримувати інформацію щодо обробки її персональних даних, зокрема, знати, кому вони передавалися (п. 8 ч. 2 ст. 8 Закону). Вказане положення вимагає від володільця зберігати інформацію щодо того, кому передаються дані суб'єкта персональних даних.

Комплексне тлумачення вказаних положень міжнародних документів та національного законодавства вказує на наявність у володільця **обов'язку детально фіксувати та документувати свою діяльність щодо обробки персональних даних**.

4. ПІДСТАВИ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

4.1. Загальні положення. Відповідно до ч. 5 ст. 6 Закону, **обробка персональних даних здійснюється виключно на підставі згоди особи або закону**.

Дане положення конкретизується статтею 11 Закону та статтею 7 Директиви та статтею 6 Регламенту. Так, стаття 11 Закону встановлює вичерпний перелік випадків та умов, за яких може здійснюватися обробка персональних даних

суб'єкта. Ця стаття є першим «фільтром» на шляху до законної обробки. Якщо обробка виходить за межі передбачених статтею 11 Закону випадків, вона автоматично розглядається як незаконна.

У цьому зв'язку слід зазначити, що статтю 11 Закону слід розглядати крізь призму положень статті 7 Директиви, положення якої вона фактично копіює.

Підстави обробки персональних даних, вказані у статті 11 Закону, умовно можна розділити на дві групи, в залежності від того, чи вони базуються на підставі згоди, чи закону.

Згода	**Закон**
1) згода суб'єкта персональних даних на обробку його персональних даних; 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.	1) дозвіл на обробку персональних даних, наданий володільцю персональних даних відповідно до закону виключно для здійснення його повноважень; 2) захист життєво важливих інтересів суб'єкта персональних даних; 3) необхідність виконання обов'язку володільця персональних даних, який передбачений законом; 4) необхідність захисту законних інтересів володільців персональних даних, третіх осіб, крім випадків, коли суб'єкт персональних даних вимагає припинити обробку його персональних даних та потреби захисту персональних даних переважають такий інтерес.

Слід зазначити, що згідно з статтею 6 Регламенту **«необхідність захисту законних інтересів» в якості підстави обробки персональних даних не може використовуватися державними органами влади** при виконанні покладених на них завдань. Хоч у Законі такого правила не має, однак з ним не можна не погодитися, оскільки державні органи зобов'язані діяти лише на підставі, в межах повноважень та у спосіб, що передбачені Конституцією та законами України. Інтерес же є суто приватноправовою категорією. Також слід зазначити, що використання державними органами згоди в якості підстави для обробки персональних даних повинно бути зведено до мінімуму. При її використанні слід враховувати, що **суб'єкт має право в будь-який час відкликати свою згоду**, після чого обробка повинна бути негайно припинена.

Вказаний перелік підстав обробки персональних даних є вичерпним.

Обробка чутливих категорій персональних даних, про які мова йшла вище, здійснюється лише у випадках та на умовах, передбачених статтею 7 Закону. Критерії законної обробки чутливих даних, визначені статтею 7 Закону, **є більш детальними та обмеженими в порівнянні з тими, що передбачені статтею 11 Закону**, та повністю ними охоплюються. Так, договір не є законною підставою для обробки чутливих категорій даних, як і законний інтерес, передбачений статтею 11.

Виходячи із вказаного вище, слід окремо наголосити на тому, що «обробка на підставі закону» та «законність (легітимність) обробки» є різними поняттями. Так, законність обробки є принципом, який передбачає, що обробка повинна здійснюватися на підставі Закону України «Про захист персональних даних» та інших законів і в порядку, визначеному законами та іншими нормативно-правовими актами, положеннями, установчими та іншими документами, які регулюють діяльність володільця. Обробка «на підставі закону» передбачає, що закон безпосередньо уповноважує володільця на обробку персональних даних та відсилає до пп. 2, 4, 5 та 6 ч. 1 ст. 11 Закону. Остання виступає по суті протилежністю обробки, що базується на підставі згоди.

4.2. Обробка на підставі згоди суб'єкта.

Згода суб'єкта персональних даних – це добровільне волевиявлення фізичної особи (за умови її поінформованості) щодо надання дозволу на обробку її персональних даних відповідно до сформульованої мети їх обробки, висловлене у письмовій формі або у формі, що дає змогу зробити висновок про надання згоди (ст. 2 Закону).

Із зазначеного видно, що для того, щоб відповідати Закону згода повинна володіти трьома невід'ємними ознаками:

- **добровільність** - відсутність прямого чи опосередкованого примусу при наданні згоди. Тому, як згідно з Конвенцією, Директивою, так і згідно з Законом (п. 11 ч. 2 ст. 8) згода суб'єкта може бути відкликана ним у будь-який час.;
- **поінформованість**: перед наданням згоди на обробку персональних даних суб'єкт повинен отримати достовірну інформацію про те, ким, з якою метою будуть оброблятися його персональні дані, кому будуть передаватися, які саме дані (склад даних), а також про права, визначені Законом (ст. 12 Закону). Така інформація повинна бути надана в доступному вигляді і володілець повинен за будь-яких умов мати можливість підтвердити факт надання такої інформації суб'єкту;
- **форма** надання згоди може бути будь-якою, однак володілець повинен мати змогу підтвердити її наявність впродовж всього часу здійснення обробки персональних даних.

Договір. Аналогічні критерії застосовуються і у випадку обробки на підставі договору. Так, правочин згідно статтею 203 Цивільного Кодексу України «волевиявлення учасника правочину має бути вільним і відповідати його внутрішній волі». Укладення договору презюмує надання згоди на обробку даних, необхідних для його виконання сторонами.

4.3. Обробка персональних даних на підставі закону.

Обробка персональних даних на підставі закону

передбачає наявність однієї з чотирьох підстав, визначених пунктами 2, 4, 5 та 6 частини 1 статті 11 Закону:

А) Дозвіл на обробку персональних даних, наданий володільцю персональних даних відповідно до закону виключно для здійснення його повноважень.

Це положення сформульовано дещо нечітко. Так, аналіз даного положення створює враження, що для здійснення кожної обробки персональних даних щоразу необхідно передбачати відповідне право законом. **Вказане трактування в Законі однозначно потребує уточнення та деталізації.**

Відповідне положення Директиви (в Регламенті формулювання не змінилось) передбачає можливість здійснення обробки, коли вона є «необхідною для виконання офіційних повноважень, якими наділений володілець чи третя сторона, якій передаються персональні дані». Саме в його світлі слід розуміти вказане положення Закону.

Відтак, якщо володілець має визначені законом повноваження, реалізація яких потребує обробки персональних даних, це вже в контексті вказаного положення Закону є достатньою підставою для їх обробки. При цьому обробці можуть підлягати лише ті дані, які є **необхідними** для досягнення цілі обробки, тобто виконання конкретних завдань/повноважень (див. роз'яснення принципу необхідності вище).

Це положення Закону дозволяє обробляти персональні дані не лише у випадках, коли на це є пряма вказівка закону (Приклад 1), а й коли це об'єктивно обумовлюється повноваженнями державного органу (Приклад 2).

Приклад 1.
Так, статтею 7 Закону України «Про очищення влади» передбачено створення Єдиного державного реєстру осіб, щодо яких застосовано положення Закону України «Про очищення влади». Вказана стаття встановлює категорії суб'єктів, персональні дані яких міститимуться у вказаному Реєстрі, порядок їх збору, склад даних, склад даних, що підлягають оприлюдненню, а також суб'єктів, яким може надаватися інформація з Реєстру та інше.

Приклад 2.
Відповідно до п. 2 ч. 1 ст. 34 Закону України «Про загальнообов'язкове державне соціальне страхування на випадок безробіття» «Фонд має право (…) перевіряти достовірність відомостей, поданих роботодавцем для отримання коштів Фонду, дотримання порядку використання роботодавцем виділених йому коштів Фонду та зупиняти виплати з Фонду в разі відмови або перешкоджання з боку роботодавця у проведенні перевірки, виявлення фактів подання ним Фонду недостовірних відомостей або порушення порядку використання роботодавцем коштів Фонду».
Очевидно, що реалізація вказаного права потребуватиме обробки персональних даних суб'єкта/ів персональних даних. Відтак, на підставі вказаного положення, а також п. 2 ч. 1 ст. 11 Закону Фонд матиме право обробляти персональні дані в *межах, які є необхідні, для реалізації вказаного повноваження.*

Вказана підстава є основною для обробки персональних даних державними органами. Слід, однак, наголосити, що дотримання вказаного положення є лише першим кроком державного органу чи органу місцевого самоврядування на шляху до законної обробки. Для того, щоб у повній мірі відповідати принципу законності, порядок обробки персональних даних такими володільцями повинен детально регламентуватися законодавством та внутрішніми документами володільця.

Саме таке розуміння відповідає положенням частини

2 статті 19 Конституції України, відповідно до якої «органи державної влади та органи місцевого самоврядування, їх посадові особи зобов'язані діяти лише на підставі, в межах повноважень та у спосіб, що передбачені конституцією та законами України».

Такий підхід відповідатиме також практиці ЄСПЛ, сформованої у рішеннях «Ротару проти Румунії», «Заіченко проти України № 2», «П.Г. та Дж.Х. проти Великобританії».

Приклад 1. Справа «Zaichenko v. Ukraine» (№ 2).

В рамках розгляду справи щодо вчинення заявником адміністративного правопорушення судом було призначено проведення стаціонарного обстеження психічного стану здоров'я заявника з метою встановлення того, чи міг заявник бути притягнутим до відповідальності. Оскільки в матеріалах справи не було матеріалів, необхідних для проведення обстеження, суд дав вказівку органам внутрішніх справ зібрати необхідну інформацію. З цією метою співробітниками міліції було опитано родичів, сусідів та друзів заявника, отримано довідку з лікарні щодо проходження заявником лікування. Суд констатував порушення прав заявника у зв'язку з відсутністю спеціальних положень законодавства, що регламентували би порядок проведення примусового обстеження (і в тому числі збоку інформації) в рамках розгляду справи про вчинення адміністративного правопорушення[8].

Приклад 2. Справа «P.G. and J.H. v. The United Kingdom».

Під час перебування у відділі поліції розмову заявників зі співробітниками поліції було записано. Зразок їх голосу було збережено для проведення експертизи (в ході якої він порівнювався з іншими зразками, які належали особам, причетним до вчинення злочину). Європейський суд з прав людини Суд зазначив, що в законодавстві Великобританії не було норм, що регламентували би процес відбору зразків голосу в приміщенні управління поліції. Тому таке використання зразків їх голосу було незаконним

8 Zaichenko v. Ukraine (no. 2), no. 45797/09, §§ 119 – 122, 26 February 2015

та порушувало їх права, гарантовані статтею 8 Конвенції[9].

Приклад 3. Справа «Авілкіна проти Росії».

В ході проведення перевірки діяльності релігійної організації свідків Єгови за скаргою, направленою ГО «Комітет спасіння молоді» (на думку ГО свідки Єгови заставляли своїх послідовників відмовлятися від переливання крові), прокуратура збирала в медичних закладів інформацію щодо свідків Єгови, які відмовилися від переливання крові. Національні суди відмовилися визнати дії прокуратури незаконними, оскільки згідно **із законом прокуратура в ході перевірки мала доступ до будь-якої інформації, в тому числі медичної**. Особи, чиї дані було зібрано, поскаржилися до Європейського суду на незаконність такої обробки.

Європейський суд підтвердив наявність передбачених законом підстав для отримання інформації. Однак, на його думку відповідні положення закону були надто загальними та не надавали достатніх гарантій проти свавільності та зловживання.

Суд вирішив дослідити правомірність збору прокуратурою інформації з точки зору принципів необхідності та пропорційності (чи було таке втручання пропорційним меті боротьби зі злочинністю). Суд відповів на це питання негативно з огляду на такі аргументи:

- особи, щодо яких проводилася перевірка не були підозрюваними, обвинуваченими (просто проводилася перевірка діяльності релігійної організації);
- медичні заклади не зверталися до суду з метою проведення примусового переливання (що можливо у випадку загрози життю), не повідомляли про вчинення злочину чи примушування релігійною організацією своїх віруючих до відмови від лікування;
- прокуратура навіть не спробувала отримати згоду пацієнтів;

9 P.G. and J.H. v. the United Kingdom, no. 44787/98, §§ 61 – 63, ECHR 2001 IX

- не було порядку реалізації повноважень прокуратури на отримання документів;
- суди переглянули скаргу заявників, однак не дослідили питання дотримання справедливого балансу між інтересами проведення перевірки та правами суб'єктів на повагу до їх приватного життя інтересів, не надали обґрунтування передачі інформації, тим самим підтвердивши необмежені повноваження прокуратури[10].

Б) Захист життєво важливих інтересів суб'єкта персональних даних. В якості прикладу можна навести ситуацію, пов'язану із наданням невідкладної медичної допомоги. Так, надання медичної допомоги за будь-яких обставин передбачає необхідність обробки даних щодо стану здоров'я особи. В разі наявності ознак прямої загрози життю особи та необхідності надання невідкладної медичної допомоги за умови неможливості отримання з об'єктивних причин згоди (наприклад, втрата свідомості) на медичне втручання від самого особи чи її законних представників, медичне втручання здійснюється за відсутності такої згоди (статті 3, 37 та 43 Закону України «Основи законодавства України про охорону здоров'я»). Відтак і обробка необхідних для цього персональних даних здійснюється за відсутності згоди особи, безпосередньо на підставі вказаного положення статті 11 Закону.

В) Необхідність виконання обов'язку володільця персональних даних, який передбачений законом.

Відповідно до вказаного положення володілець може здійснювати обробку виключно тих персональних даних суб'єктів, які є необхідними для виконання ним свого обов'язку, передбаченого законом. При цьому, за загальним правилом, володілець самостійно вирішує, виходячи з покладених на нього обов'язків, чи потребує він для їх здійснення обробки персональних даних суб'єктів.

Вказана підстава перетинається із підставою, передбаченою п. 2 ч. 1 ст. 11 Закону, де мова йде про обробку у зв'язку з необхідністю виконання повноважень

10 Avilkina and Others v. Russia, no. 1585/09, 6 June 2013.

(тобто прав та **обов'язків**). Така плутанина спричинена невдалим копіюванням положень Директиви в національне законодавство: слово «task», що означає «завдання», яке використовується в Директиві та Регламенті, неправильно перекладено, як «повноваження». Тому здійснення обробки у зв'язку з виконанням повноважень (прав та обов'язків) частково перетинається із такою підставою, як обробка з метою виконання обов'язку, а саме в частині, що стосується обробки персональних даних державним органом з метою виконання **обов'язків**. Однак, як вже зазначалося вище, підстава, передбачена п. 2 ч. 1 ст. 11 Закону (щодо повноважень), стосується в основному діяльності державних органів, а підстава, передбачена п. 5 ч. 1 ст. 11 Закону (необхідність виконання обов'язку), стосується *також інших* володільців – суб'єктів приватноправових відносин.

Приклад.
Підприємство отримує запит від правоохоронного органу, у якому останній запитує персональні дані одного з працівників. Законом передбачено обов'язок суб'єктів, які отримують запит, надавати інформацію впродовж визначеного у ньому строку. Вказані відомості необхідні для розслідування злочину в рамках порушеного кримінального провадження. У такому випадку підприємство **зобов'язане** надати таку інформацію. Підставою передачі персональних буде необхідність виконання обов'язку передбаченого законом.

Г) Необхідність захисту законних інтересів володільців персональних даних, третіх осіб, окрім випадків, коли суб'єкт персональних даних вимагає припинити обробку його персональних даних та потреби захисту персональних даних переважають такий інтерес;

Вказана підстава не застосовується до роботи державних органів влади, а відтак не розглядатиметься детально у даній праці. Достатньо зазначити, що як уже зазначалося вище, суб'єкти, що не є державними органами, у своїй діяльності керуються не лише правами, визначеними

законом, а й законними інтересами. Класичним прикладом законного інтересу у сфері захисту персональних даних є прямий маркетинг. Прагнення просувати свої товари шляхом направлення повідомлення потенційним споживачам не є правом, гарантованим законом, як і не є ним заборонено, а тому воно є інтересом.

4.4. Підстави обробки чутливих категорій персональних даних.

За загальним правилом забороняється обробка чутливих категорій персональних даних: про расове або етнічне походження, політичні, релігійні або 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.

Разом з тим ч. 2 ст. 7 Закону, як і ст. 8 Директиви та ст. 9 Регламенту, встановлює вичерпний перелік випадків, у яких дозволяється обробляти чутливі дані. Вказане відповідає і положенням ст. 6 Конвенції, яка окремо виділяє чутливі категорії даних та вимагає, щоб їх обробка забезпечувалася відповідними гарантіями. Надалі більш детально розглядатимуться ті підстави, що мають вагоме значення для роботи державних органів.

Відповідно до частиною 2 статті 7 Закону дозволяється обробка чутливих категорій даних, якщо вона:

1) здійснюється за умови надання суб'єктом персональних даних однозначної згоди на обробку таких даних;

Різниця між цим та вказаним вище положенням статті 11 Закону в тому, що для того, щоб здійснювати обробку чутливих категорій даних, необхідна *однозначна* згода особи. Тлумачний словник визначає слово «*однозначний*» як такий, що має тільки одне значення. Аналогічна термінологія використовується і в Директиві. Таким чином, мається на увазі, що надання згоди має бути таким, що не викликає жодних сумнівів у її наданні.

2) необхідна для здійснення прав та виконання обов'язків володільця у сфері трудових правовідносин відповідно до закону із забезпеченням відповідного захисту;

Першою і найбільш важливою умовою для застосування вказаного положення є **наявність норми закону**, яка дозволяє збирати такі дані в цілях реалізації прав та обов'язків у сфері трудових відносин. Лише після цього оцінюється **необхідність** обробки таких даних для реалізації відповідних прав та обов'язків володільця, зокрема, чи можна було досягнути тих же цілей не вдаючись до обробки чутливих категорій даних.

Прикладом такої підстави обробки чутливих категорій персональних даних є ч. 2 ст. 24 Кодексу законів про працю України (КЗПУ), відповідно до якої «при укладенні трудового договору громадянин зобов'язаний подати (…) у випадках, передбачених законодавством, – також документ (…) про стан здоров'я (…)». Відтак, п. 2 ч. 2 ст. 7 Закону в поєднанні з вказаним положенням КЗПУ та передбаченими ним положеннями законодавства (наприклад, постанова Кабінету Міністрів України від 25 травня 1998 року № 731 «Про затвердження Порядку ведення особових справ державних службовців в органах виконавчої влади» п.п. 2-1 п. 2 ч. 1 – в особовій справі повинні міститися такі документи: (…) медична довідка про стан здоров'я за формою, встановленою МОЗ) є підставою для обробки медичної інформації про особу в цілях реалізації прав та обов'язків у сфері трудових відносин. При цьому оброблятися можуть лише ті дані, що необхідні для досягнення вказаної мети, і лише за умови забезпечення відповідного захисту.

3) необхідна для захисту життєво важливих інтересів суб'єкта персональних даних або іншої особи у разі недієздатності або обмеження цивільної дієздатності суб'єкта персональних даних;

Це положення фактично є аналогом п. 4 ч. 1 ст. 11 Закону.

4) здійснюється із забезпеченням відповідного захисту релігійною організацією, громадською організацією світоглядної спрямованості, політичною партією або професійною спілкою, що створені відповідно до закону, за умови, що обробка стосується виключно персональних даних членів цих об'єднань або осіб, які підтримують постійні контакти з ними у зв'язку з характером їх діяльності, та персональні дані не передаються третій особі

без згоди суб'єктів персональних даних;

Вказане положення дозволяє законно діючим релігійним організаціям, громадським організаціям світоглядної спрямованості, політичним партіям або професійним спілкам обробляти інформацію щодо своїх членів. При цьому будь-яка передача таких даних можлива лише за наявності згоди члена (а також в інших випадках, передбачених частиною 2 статті 7 Закону, наприклад в цілях контррозвідувальної діяльності, боротьби з тероризмом, захисту правової вимоги та інше).

Див., наприклад рішення ЄСПЛ у справі «Авілкіна проти Росії» вище.

5) необхідна для обґрунтування, задоволення або захисту правової вимоги;

Відповідно до вказаного положення дозволяється обробка чутливих даних для захисту інтересів володільця в ході, наприклад, судового провадження. При цьому, саме суд вирішує, наскільки така інформація є необхідною (зокрема, чи є наданий доказ допустимим/належним) та приймає рішення щодо її долучення до матеріалів справи.

Слід зазначити, що згідно з практикою Європейського суду при наданні сторонами в якості доказів, документів, що містять персональні дані інших осіб, навіть якщо такі відомості мають певне значення для справи не повинно автоматично тягнути за собою їх приєднання до матеріалів справи, а тим паче висвітлення в тексті рішення суду.

Приклад. Справа «L.L. v. France»[11].

Дружина заявника порушила провадження щодо розлучення. В рамках провадження вона надала суду в якості доказів того, що неодноразово зазнавала фізичного насильства з боку чоловіка, численні медичні довідки. Крім цього, вона стверджувала, що причиною такої агресивної поведінки була алкогольна залежність її чоловіка. В якості підтвердження алкогольної залежності вона надала суду свідчення двох сестер заявника та лист, направлений хірургом, який проводив операцію заявнику, терапевту заявника. У листі йшлося про те, що у якому йшлося про те, що заявник страждав панкреатитом «на фоні алкоголізму» та, що наслідки панкреатиту можна було б усунути лише, якщо заявник припинить зловживати алкоголем. Суди задовольнили позов та виклали зміст вказаного листа у тексті рішення суду.

Заявник стверджував, що виклад змісту вказаного листа у тексті рішення суду становив порушення його права на захист персональних даних.

Суд зазначив, що виклавши у своєму рішенні зміст вказаного листа національний суд розкрив та поширив детальну інформацію щодо стану здоров'я заявника. Так, хоч засідання і не було публічним, однак згідно з національними законодавством будь-яка особа без пояснення причин могла отримати копію вказаного рішення національного суду.

Суд вказав, що такі дії національного суду відповідали домашньому законодавству, згідно з яким будь-який документ, за винятком низки випадків, під які дана ситуація не потрапляла, міг бути використаний в якості доказу. Заявнику було також надано можливість надати коментарі щодо вагомості такого доказу.

Дослідження даного документу також переслідувало легітимну мету – «захист прав та свобод інших осіб», а саме права дружини заявника подавати докази для підтвердження свого позову.

Разом з тим, Суд зазначив, що вказаний лист був лише

11 L.L. v. France, no. 7508/02, ECHR 2006 XI

вторинним доказом і що тих же висновків можна було б досягнути без його використання. Відтак, використання вказаного листа не було необхідним та пропорційним в світлі поставленої мети його використання – «захисту прав та свобод інших осіб».
Додатково Суд вказав, що домашнє законодавство не надавало достатніх гарантій при використанні інформації приватного характеру в ході таких судових проваджень.

6) необхідна в цілях охорони здоров'я, встановлення медичного діагнозу, для забезпечення піклування чи лікування або надання медичних послуг, функціонування електронної системи охорони здоров'я за умови, що такі дані обробляються медичним працівником або іншою особою закладу охорони здоров'я чи фізичною особою - підприємцем, яка одержала ліцензію на провадження господарської діяльності з медичної практики, та її працівниками, на яких покладено обов'язки щодо забезпечення захисту персональних даних та на яких поширюється дія законодавства про лікарську таємницю, працівниками центрального органу виконавчої влади, що реалізує державну політику у сфері державних фінансових гарантій медичного обслуговування населення, на яких покладено обов'язки щодо забезпечення захисту персональних даних;

Дане положення є очевидним та не потребує додаткових коментарів. Певні зауваження викладено в кінці даного розділу.

В частині, що стосується підстав обробки медичної інформації слід звернутися до рішень Європейського суду з прав людини у справах «L.H. v. Latvia», «Avilkina and others v. Russia», «I. v. Finland», «Z. v. Finland», короткий виклад яких надано в попередніх розділах.

7) стосується вироків суду, виконання завдань оперативно-розшукової чи контррозвідувальної діяльності, боротьби з тероризмом та здійснюється державним органом в межах його повноважень, визначених законом;

Ця підстава видається очевидною, однак виникають певні запитання, пов'язані із формулюванням «стосується

вироків суду». Виходячи з актуального стану справ, його слід розуміти як таке, в якому мова йде не лише про персональні дані, вказані в тексті вироку, а й про ті, що стосуються кримінального провадження загалом, однак варто сформулювати дане положення в цій частині чіткіше.

Також, видається доцільним доповнити перелік також поняттям, адміністративних правопорушень, оскільки оформлення матеріалів щодо вчинення низки адміністративних правопорушень неодмінно потребуватимуть обробки чутливих категорій даних. Наприклад, ухилення від медичного огляду чи медичного обстеження (стаття 44-1 КУпАП), ухилення від обстеження і профілактичного лікування осіб, хворих на венеричну хворобу (стаття 45 КУпАП), керування транспортними засобами або суднами особами, які перебувають в стані алкогольного, наркотичного чи іншого сп'яніння або під впливом лікарських препаратів, що знижують їх увагу та швидкість реакції (стаття 130 КУпАП) тощо.

8) стосується даних, які були явно оприлюднені суб'єктом персональних даних.

Традиційно оприлюднення суб'єктом інформації щодо себе розглядається як надання ним імпліцитної згоди на обробку його персональних даних невизначеним колом суб'єктів. При цьому, володілець, що має намір здійснювати обробку оприлюдненої інформації про особу, повинен переконатися у тому, що така особа дійсно надала згоду. В іншому випадку обробка ним персональних даних суб'єкта буде вважатися незаконною.

У цій частині однак, слід зазначити, що вказане положення не можна тлумачити, як таке, що надає право на обробку оприлюднених персональних даних державними органами влади, якщо така обробка не передбачена їх повноваженнями чи іншими легітимними підставами (див. вище).

•••

Однак, слід наголосити, що в певних аспектах стаття 7 Закону містить суттєві прогалини.

Так, виходячи з положень вказаної статті відсутні законні підстави для обробки, наприклад, інформації щодо стану здоров'я в цілях соціального захисту, страхування та

пенсійного забезпечення. Такий стан справ суперечить реаліям.

Приклад.
Згідно з пунктом 8 постанови КМУ № 121 від 16 лютого 2011 року «Про затвердження Положення про централізований банк даних з проблем інвалідності» до повноважень структурних підрозділів з питань соціального захисту населення районних, районних у мм. Києві та Севастополі держадміністрацій, виконавчих органів міських, районних у містах рад належить, серед іншого, «право внесення до банку даних відомостей про видачу особам з інвалідністю та дітям з інвалідністю технічних та інших засобів реабілітації; працевлаштування осіб з інвалідністю; здійснення перегляду загальних відомостей про осіб з інвалідністю та дітей з інвалідністю, рівень доходів їх сімей, направлень на отримання технічних та інших засобів реабілітації, даних про санаторно-курортне лікування, виплату грошової компенсації замість санаторно-курортної путівки, надання матеріальної допомоги, а також відомостей про дієздатність осіб тощо;(…)».

Навіть ширше тлумачення положень даної статті не виправляє ситуацію. Так, обробка в цілях «соціального захисту, страхування та пенсійного забезпечення та ін.» частково потрапляє в сферу охорони здоров'я. Відтак, обробка персональних даних в таких цілях могло би здійснюватися на підставі пункту 6 частини 2 статті 7 Закону (див. вище). Однак, дане положення має досить вузьке застосування, оскільки на вказаній підставі чутливі дані можуть оброблятися лише «**медичним працівником або іншою особою закладу охорони здоров'я** чи **фізичною особою - підприємцем**, яка одержала ліцензію на провадження господарської діяльності з медичної практики, **та її працівниками**» та «**працівниками центрального органу виконавчої влади**, що реалізує державну політику у сфері державних фінансових гарантій медичного обслуговування населення, на яких покладено обов'язки щодо забезпечення захисту персональних даних». Працівники органів соціального захисту не потрапляють в жодну категорію. При цьому, таких обмежень до обробки

чутливих даних в цілях охорони здоров'я не має ні в Директиві[12], з якої дане положення скопійовано, ні в Регламенті.

Відтак можна стверджувати про потребу в перегляді статті 7 Закону.

Разом з тим, не можна вважати усі ситуації обробки чутливих категорій персональних даних, що не охоплюються статтею 7 Закону, незаконними. Так, статтею 25 Закону передбачено можливість відступу, серед іншого, від положень статті 7 Закону, якщо це: 1) передбачено законом; 2) необхідно/пропорційно; 3) переслідує одну з легітимних цілей: національної безпеки, економічного добробуту або захисту прав і свобод суб'єктів персональних даних чи інших осіб.

Отже, якщо дотримано трьох вказаних вище умов обробка чутливих категорій персональних даних дозволяється навіть у тих випадках, коли це не передбачено статтею 7 Закону.

Приклад. Позиція Уповноваженого ВРУ з прав людини.

Виконавча дирекція Фонду соціального страхування з тимчасової втрати працездатності (далі – Виконавча дирекція Фонду) звернулася до медичного закладу з вимогою надати доступ до медичних документів, що стали підставою для видачі особі листка непрацездатності, з метою перевірки обґрунтованості його видачі, а відтак і наявності підстав для нарахування відповідних виплат. Лікарня у доступі відмовила, у зв'язку з чим Виконавча дирекція Фонду звернулася до Уповноваженого за роз'ясненням щодо правомірності отримання запитуваної інформації. За результатами розгляду зазначеного звернення Уповноважений зазначив про таке.

12 Так, згідно з Директивою «Держави-члени забороняють обробку персональних даних (…), що стосуються здоров'я та статевого життя. 3. Частина 1 не застосовуватиметься там, де обробка персональних даних необхідна для цілей превентивної медицини, діагностики, забезпечення догляду чи допомоги або надання медичних послуг, та ці дані обробляються спеціалістом-медиком, на якого згідно з національним законодавством чи правилами, прийнятими компетентними національними органами, поширюється зобов'язання щодо збереження професійної таємниці, чи іншою особою, на яку поширюються еквівалентні зобов'язання щодо конфіденційності».

Персональні дані щодо стану здоров'я Законом України «Про захист персональних даних» (далі – Закон) віднесені до категорії так званих «чутливих» персональних даних. Статтею 7 Закону встановлено вичерпний перелік випадків щодо того, коли і ким може здійснюватися обробка таких персональних даних. Викладена у листі Фонду ситуація не потрапляє до вказаного переліку.

Водночас статтею 25 Закону визначено, що обмеження дії статей 6, 7 і 8 цього Закону може здійснюватися у **випадках, передбачених законом**, **наскільки це необхідно** у демократичному суспільстві **в інтересах національної безпеки, економічного добробуту або захисту прав і свобод суб'єктів персональних даних чи інших осіб**.

Комплексний аналіз статей 7 та 25 Закону свідчить про те, що за умови дотримання положень частини першої статті 25 Закону (див. вище) інформація про стан здоров'я може оброблятися навіть у ситуації, що не входить до переліку, викладеного в частині другій статті 7 Закону.

Законом України «Про загальнообов'язкове державне соціальне страхування» визначено, що Фонд соціального страхування України є органом, який здійснює (…) контроль за використанням коштів, забезпечує фінансування виплат за цими видами загальнообов'язкового державного соціального страхування (…).

Згідно із статтею 31 Закону України «Про загальнообов'язкове державне соціальне страхування» підставою для призначення допомоги по тимчасовій непрацездатності є виданий у встановленому порядку листок непрацездатності.

Відповідно до статті 9 зазначеного Закону здійснення перевірки обґрунтованості видачі та продовження листків непрацездатності застрахованим особам є одним із основних завдань Фонду соціального страхування України та його робочих органів. З цією метою Фонд має право розслідування страхових випадків та обґрунтованості виплати матеріального забезпечення, страхових виплат. Відповідно до статті 10 Фонд має право перевіряти достовірність відомостей, поданих роботодавцем для

отримання коштів Фонду.

Таким чином, на законодавчому рівні визначено право Фонду перевіряти обґрунтованість видачі та продовження листків непрацездатності застрахованим особам з метою забезпечення контролю за цільовим та раціональним використанням коштів Фонду. При цьому доступ до низки персональних даних щодо стану здоров'я застрахованої особи є об'єктивною необхідністю, оскільки саме ця інформація дозволяє визначити обґрунтованість видачі та продовження листків непрацездатності, які є підставою для виплати коштів.

Таким чином, надання Фонду доступу до тих персональних даних особи, **які є необхідними** для перевірки обґрунтованості видачі та продовження листків непрацездатності, відповідатиме вимогам Закону України «Про захист персональних даних».

5. ПРАВА СУБ'ЄКТА ПЕРСОНАЛЬНИХ ДАНИХ.

5.1. Право суб'єкта персональних даних на отримання інформації щодо обробки його персональних даних. Володілець персональних даних згідно із Законом зобов'язаний автоматично надавати суб'єкту певну інформацію про обробку його персональних даних.

Так, відповідно до частини 2 статті 12 Закону суб'єкт персональних даних повідомляється про: 1) володільця персональних даних, 2) склад та 3) зміст зібраних персональних даних, 4) свої права, визначені Законом, 5) мету збору персональних даних та 6) осіб, яким передаються його персональні дані.

Дане зобов'язання володільця пов'язане з правами суб'єкта персональних даних, закріпленими у статті 8 Закону, знати про обробку його персональних даних та зміст таких даних.

Воно є запорукою дотримання інших прав, а саме права доступу до своїх персональних даних, оскільки якщо суб'єкт не знає про те, що його персональні дані можуть оброблятися конкретним володільцем, у нього не буде причин звертатися до

останнього (зокрема з метою захисту своїх прав).
Інформація, вказана у статті 12, повідомляється суб'єкту в момент збору персональних даних, якщо персональні дані збираються у суб'єкта персональних даних, або протягом тридцяти робочих днів із дня збору персональних даних в інших випадках.

Це положення сформульовано без усяких застережень, у зв'язку з чим на перший погляд видається, що кожен володілець зобов'язаний повідомляти кожного суб'єкта про обробку його персональних даних. Однак, така ситуація є нелогічною. Важко уявити, щоб у процесі здійснення оперативно-розшукової діяльності чи кримінального провадження, в ході яких збирається інформація про суб'єкта, правоохоронні органи повинні були би повідомляти його про це. Так само нелогічно, щоб суб'єкт повідомлявся про збір інформації іншими державними органами влади чи під час проведення наукового дослідження, коли наприклад науковець досліджує в архіві медичну документацію (інколи це сотні справ) суб'єктів тощо. У першому випадку збір інформації здійснюється зазвичай таємно, у другому – право збирати інформацію про особу зазвичай передбачено нормативно-правовими актами, що регламентують роботу відповідного органу влади та є в загальному доступі, а у третьому – науковець потратив би дуже багато часу на повідомлення всіх суб'єктів. Таких прикладів доволі багато.

Слід зазначити, що європейські документи з питань захисту персональних даних, які містять положення про автоматичне повідомлення суб'єкта про обробку його персональних даних, зазвичай передбачають також і винятки з цих зобов'язань. Так, як стаття 10, так і 11 Директиви вказують на те, що повідомляти про порядок обробки непотрібно, якщо суб'єкту і так відома ця інформація[13]. Також є певні обмеження щодо повідомлення суб'єкта, коли інформація збирається в наукових, статистичних чи історичних цілях. Регламент

13 Тут варто зазначити, що положення Директиви не застосовуються до обробки персональних даних у сфері оборони, національної безпеки та розслідування злочинів.

містить більш детальні винятки[14].

Закон, а саме статтю 12, слід доповнити певними винятками з обов'язку повідомляти суб'єкта про збір інформації щодо нього. Разом із тим, хоч такі винятки відсутні станом на сьогодні, це не означає, що кожен володілець зобов'язаний повідомляти суб'єкта про збір інформації щодо нього.

Так, стаття 12 Закону є лише результатом деталізації прав особи, гарантованих статтею 8 Закону. Стаття 25 передбачає можливість обмеження дії статті 8 Закону, якщо це передбачено законом та необхідно для досягнення визначених вказаним положенням цілей. Комплексний аналіз статей 8, 12 та 25 Закону дає підстави вважати, що ті ж обмеження, що можуть застосовуватися до статті 8 Закону, слід застосовувати автоматично і до інших положень, що є результатом її деталізації, і в тому числі статті 12. В іншому випадку обмеження дії статті 8 Закону втратило би будь-який сенс.

Відтак, якщо інші закони встановлюють окремий порядок (більш обмежувальний, наприклад) повідомлення суб'єкта про збір інформації щодо нього і при цьому відповідають вимогам статті 25 Закону, повинні застосовуватися саме положення таких законів. Яскравим прикладом є положення Кримінального процесуального кодексу України, відповідно до яким підозрюваний ознайомлюється зі всіма матеріалами провадження після завершення досудового розслідування.

В інших випадках (коли відсутні обмеження щодо обов'язку повідомляти) до того часу, як будуть внесені відповідні зміни до Закону, інформація, зазначена у статті 12 Закону повинна надаватися суб'єктам в межах визначених у ній строків[15].

---

14 Якщо персональні дані отримуються від суб'єкта: суб'єкту вже відома інформація, що підлягає обов'язковому повідомленню

Якщо персональні дані отримано не від суб'єкта: суб'єкту вже відома інформація, що підлягає обов'язковому повідомленню; повідомлення потребуватиме прикладення надмірних зусиль з боку володільця; збір чи розкриття персональних даних передбачено законом; якщо згідно із законодавством персональні дані повинні залишатися конфіденційними.

15 При цьому слід зазначити, що як Директива, так і Регламент містять більш гнучкі положення в частині, що стосується строків повідомлення.

У зв'язку з цим постає ще одне запитання, а саме щодо форми повідомлення. Закон визначає зобов'язання щодо сповіщення кожного суб'єкта про обробку, однак не встановлює форми не встановлює. Однак, зрозуміло, що за певних умов таке зобов'язання буде надмірним. Тому допускається вжиття різних способів повідомлення, зокрема, отримання підтвердження повідомлення від самого суб'єкта чи шляхом направлення односторонніх повідомлень, чи розміщення інформації на веб-сайтах.

Також, слід зазначити, що **саме на володільцю лежить тягар доведення того, що він вжив усіх можливих заходів з метою повідомлення суб'єктів про збір інформації щодо них**. Наприклад, така інформація повинна бути надана контролюючому органу в ході перевірки. Її відсутність свідчитиме про невиконання володільцем своїх зобов'язань, закріплених у ст. 12 Закону.

Крім цього, відповідно до частини першої статті 21 Закону володілець персональних даних протягом десяти робочих днів зобов'язаний повідомляти суб'єкта персональних даних про передачу персональних даних третій особі, якщо цього вимагають умови його згоди або інше не передбачено законом.

При цьому частиною другою статті 21 передбачено виключення з вказаного правила у разі: «1) передачі персональних даних за запитами при виконанні завдань оперативно-розшукової чи контррозвідувальної діяльності, боротьби з тероризмом; 2) виконання органами державної влади та органами місцевого самоврядування своїх повноважень, передбачених законом; 3) здійснення обробки персональних даних в історичних, статистичних чи наукових цілях; 4) повідомлення суб'єкта персональних даних відповідно до вимог частини другої статті 12 цього Закону».

Вказане положення у Законі є зайвим і його слід видалити. Такі зобов'язання на володільців не покладаються жодним міжнародним документом. І це абсолютно правильно, оскільки, якщо розглядати статтю 12 та 21 в комплексі, виходить,

що як первісний володілець (який передає персональні дані), так і новий володілець (той, хто отримує, а в розумінні статті 12 Закону – збирає персональні дані) зобов'язані повідомляти суб'єкта про вчинення однієї і тієї самої операції з його персональними даними. Такий стан справ бюрократизує процес обробки та накладає надмірний та непотрібний тягар на володільців персональних даних.

При цьому, положення частини другої статті 21 Закону можна використати при підготовці застережень до статті 12 Закону, про що мова йшла вище.

Щодо третьої частини статті 21 Закону, відповідно до якої «про зміну, видалення чи знищення персональних даних або обмеження доступу до них володілець персональних даних протягом десяти робочих днів повідомляє суб'єкта персональних даних, а також суб'єктів відносин, пов'язаних із персональними даними, яким ці дані було передано», **слід зазначити, що вказане положення слід суттєво доопрацювати**.

По-перше, жодних зобов'язань такого характеру не міститься в основних міжнародно-правових документах. По-друге, обов'язок повідомляти про кожну дію з персональними даними видається надмірним, практично нереальним тягарем на володільця. Фактично працівники володільця зобов'язані будуть повідомляти про кожну свою дію з персональними даними. По-третє, таке зобов'язання не є насправді потрібним. Так, **основна мета передбаченого статтею 12 Закону зобов'язання володільця – повідомляти про збір персональних даних суб'єкта – полягає в тому, щоб дати можливість суб'єкту орієнтуватися про, так би мовити, «ареал» поширення його персональних даних**. Знаючи, хто здійснює їх обробку, та володіючи достатнім об'ємом інформації про порядок такої обробки (див. статтю 12 Закону), суб'єкт може реалізувати решту своїх прав, гарантованих статтею 8 Закону. Наявність одного лише положення статті 12, за умови його ретельного дотримання належним чином, збалансовує з одного боку інтереси суб'єкта (він знає, хто

обробляє його персональні дані), а з другого – володільця (немає зайвих «формальних» навантажень у вигляді звітування про кожну дрібницю перед суб'єктом). Із цих міркувань, зобов'язання, передбаченого статтею 12 Закону (за умови надання йому певної гнучкості), абсолютно достатньо для того, щоб забезпечити принцип прозорості обробки.

Щодо частини третьої статті 21 Закону, в чинній редакції слід констатувати відсутність доцільності в її дотриманні володільцями.

5.2. Право на доступ до своїх персональних даних.

Суб'єкт персональних даних має право отримати у відповідь на запит інформацію щодо володільця, факту обробки його даних, порядку обробки, складу та змісту його даних.

Так, відповідно до ст. 8 Закону суб'єкт персональних даних має право:

«1) знати про джерела збирання, місцезнаходження своїх персональних даних, мету їх обробки, місцезнаходження або місце проживання (перебування) володільця чи розпорядника персональних даних або дати відповідне доручення щодо отримання цієї інформації уповноваженим ним особам, крім випадків, встановлених законом;

2) отримувати інформацію про умови надання доступу до персональних даних, зокрема інформацію про третіх осіб, яким передаються його персональні дані;

3) на доступ до своїх персональних даних;

4) отримувати не пізніш як за тридцять календарних днів з дня надходження запиту, крім випадків, передбачених законом, відповідь про те, чи обробляються його персональні дані, а також отримувати зміст таких персональних даних.

Із вказаного, а також принципу законності обробки, логічно випливає, що **володілець повинен бути готовим в будь-який момент надати суб'єкту інформацію про те, на яких підставах (законних) здійснюється обробка його персональних даних**, а відтак і мати можливість пред'явити відповідний договір, документ, що засвідчує надання суб'єктом згоди, чи нормативно-правовий акт, що дає йому

право обробляти персональні дані певного суб'єкта.

Важливим питанням є доступ до інформації про джерела отримання персональних даних. Надання володільцем такої інформації пов'язане з запорукою дотримання принципу законності обробки. Так, лише надавши підтверджені доказами відомості про джерела отримання персональних даних, володілець зможе підтвердити законність їх обробки.

Загалом вказані положення є достатньо чіткими та передбачуваними. Певні суперечності викликає лише пункт 2 частини другої статті 8 Закону, відповідно до якого суб'єкт має право «отримувати інформацію про умови надання доступу до персональних даних, **зокрема інформацію про третіх осіб, яким передаються його персональні дані**». Часто вказане положення розуміється як таке, що стосується лише майбутніх можливих операцій із персональними даними. Насправді практика європейських держав[16], свідчить про те, що **суб'єкт має право на отримання відомостей про всі операції, які здійснюються з його персональними даними** (крім випадків, коли доступ до такої інформації обмежено законом).

Так, у Директиві аналогічне право суб'єктів закріплене в статті 12 (а), відповідно до якої «Держави-члени гарантують кожному суб'єкту персональних даних право отримувати від володільця (а) без обмежень із розумними інтервалами та без надмірної затримки чи затрат (…) як мінімум інформацію щодо (…) отримувачів та категорій отримувачів, кому розкривають дані». У справі «Мер і члени міської ради Роттердаму проти М.Е.Е. Ріджкебура»[17] Суд Європейського Союзу надав тлумачення вказаного положення Директиви. Суд вирішував питання про те, чи повинне вказане право (отримувати інформацію про одержувачів персональних даних суб'єкта) обмежуватися періодом в один рік перед поданням суб'єктом запиту щодо отримання такої інформації. Суд вирішив, що «це право повинне обов'язково стосуватися минулого. Якби це було не так, суб'єкт персональних даних не зміг би ефективно реалізувати своє право на те, щоб його дані вважалися

16 Як і багато інших положень Закону воно було взято з Директиви, а саме статті 12 (а)

17 CJEU, C-553/07, College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer, 7 May 2009.

незаконно або неправильно виправленими, стертими чи заблокованими, або на подання позову до суду та отримання компенсації за завдані збитки». **Таким чином, володілець повинен автоматично зберігати інформацію про те, кому передавалися персональні дані суб'єкта, та за загальним правилом надавати її суб'єкту в разі його звернення**.

Більш детально порядок реалізації права на доступ до своїх персональних даних викладено в статті 16 Закону (порядок доступу суб'єкта до інформації про себе). Так, частиною шостою вказаного положення визначено, що суб'єкт персональних даних має право на одержання будь-яких відомостей про себе у будь-якого суб'єкта відносин, пов'язаних із персональними даними, за умови надання інформації, визначеної у пункті 1 частини четвертої цієї статті Закону (прізвище, ім'я та по батькові, місце проживання (місце перебування) і реквізити документа, що посвідчує фізичну особу, яка подає запит), окрім випадків, установлених законом.

Це положення в такому вигляді як воно є зараз видається недостатньо чітким та не забезпечує в повній мірі прав суб'єкта на захист його персональних даних від незаконного доступу.

Призначення інформації, про яку йде мова у статті 16 Закону,[18] – допомогти володільцю знайти та надати правильні персональні дані (тобто дані особи запитувача). Однак, ця інформація надає лише мінімальні гарантії верифікації особи запитувача у випадку звернення в письмовому чи електронному вигляді (чи навіть особисто, але без пред'явлення документа, що посвідчує особу).

Так, не виникає запитань у випадку особистого звернення суб'єкта, оскільки працівники володільця перевіряють документ, що посвідчує особу суб'єкта, та надають йому необхідну інформацію. Однак, на практиці більшість суб'єктів звертаються з письмовими запитами, у яких вказують зазначену у частині шостій статті 16 Закону інформацію, та вимагають надати доступ до їх персональних даних. Якщо інформація не носить чутливий характер, вона надається. Разом із тим, важко уявити ситуацію, коли суб'єкт звертається із письмовим запитом щодо отримання, наприклад,

18 Прізвище, ім'я та по батькові, місце проживання (місце перебування) і реквізити документа, що посвідчує фізичну особу, яка подає запит.

чутливої медичної інформації про себе і вона йому надається адміністрацією медичного закладу. Те саме стосується й інших видів чутливої інформації, наприклад тієї, що є в розпорядженні правоохоронних органів, телекомунікаційних компаній, банків тощо.

Частина шоста статті 16 Закону містить застереження про те, що суб'єкт має право на одержання будь-яких відомостей про себе за умови надання вказаних даних «**крім випадків, установлених законом**». Вказане обмеження перш за все слід розуміти таким чином, що 1) закон може в принципі позбавляти особу доступу до її персональних даних (що в принципі узгоджується з частиною першою статті 25 Закону), а також, що 2) закон може встановлювати інші вимоги щодо об'єму інформації, яка повинна надаватися суб'єктом для отримання доступу. Однак, по-перше, на даний момент далеко не всі галузеві закони містять положення щодо порядку доступу до персональних даних у відповідній сфері (наприклад, медицина, правоохоронна діяльність, телекомунікації та інше), а по-друге, це не вирішує питання щодо форми запиту та відповіді.

Відтак, положення щодо порядку доступу суб'єкта до його персональних даних повинні, з урахуванням характеру даних та особливостей певної сфери обробки, включати вимоги щодо форми запиту та відповіді (письмова, електронна, усна тощо), умов, за яких запитувана інформація надається, заходи щодо ідентифікації особи запитувача. В якості альтернативи Закон повинен делегувати такі повноваження володільцям, які повинні тоді будуть самостійно з урахуванням персональних даних, що ними обробляються, розробляти процедуру доступу, яка повинна бути загальнодоступною.

На разі питання умов надання доступу до персональних даних суб'єкта повинно вирішуватися володільцем виходячи з тлумачення Закону, законодавства, що регламентує діяльність володільця та характеру персональних, доступ до яких запитується.

В якості прикладу можна навести практику застосування вказаного положення Уповноваженим ВРУ з прав людини.

Приклад. Практика розгляду скарг Уповноваженим ВРУ з прав людини.

До Уповноваженого надійшла скарга заявника щодо відмови надати йому інформацію про особу, яка робила щеплення його дитині, через ненадання ним копій документів, а саме ксерокопії паспорта, свідоцтва про шлюб, свідоцтва про народження дитини (заявник направляв письмовий запит).

Частиною 1 статті 242 Цивільного кодексу України визначено, що батьки (усиновлювачі) є законними представниками своїх малолітніх та неповнолітніх дітей. Стаття 43 Закону України «Про нотаріат» зазначає, що особа віком до 16 років встановлюється за свідоцтвом про народження за умови підтвердження батьками (одним з батьків) того, що ця особа є їх дитиною.

Відповідно до ч. 6 ст. 16 Закону України «Про захист персональних даних» (далі – Закон), суб'єкт персональних даних має право на одержання будь-яких відомостей про себе у будь-якого суб'єкта відносин, пов'язаних із персональними даними, за умови надання інформації, визначеної у пункті 1 частини 4 цієї статті, крім випадків, установлених законом.

Відповідно до пункту 1 частини 4 статті 16 цього Закону у запиті щодо доступу до персональних даних зазначаються: прізвище, ім'я та по батькові, місце проживання (місце перебування) і реквізити документа, що посвідчує фізичну особу, яка подає запит (для фізичної особи – заявника).

Згідно із пунктом 8 частини 1 статті 7 Закону «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус», до реквізитів виданого особі документа належать: тип, назва документа, серія, номер, дата видачі та уповноважений суб'єкт, що видав документ, строк дії документа.

Крім цього, якщо мова йде про отримання відомостей про особу її законним представником, він повинен підтвердити наявність у нього таких повноважень. Так, відповідно до ст. 42 Цивільного процесуального Кодексу повноваження законних представників мають бути посвідчені, серед іншого, свідоцтвом про народження дитини.

Отже, для отримання запитуваної інформації про доньку, заявнику у своєму запиті до лікарні необхідно було вказати реквізити документа, що посвідчує його особу, а також підтвердити наявність у нього відповідних повноважень свідоцтвом про народження дитини. При цьому законодавством не визначено форми такого підтвердження. Вимога надати копії зазначених документів та копії свідоцтва про шлюб не передбачена чинним законодавством України. Водночас слід взяти до уваги, що відповідно до статті 24 Закону володілець персональних даних (у даному випадку – пологовий будинок) зобов'язаний забезпечити захист цих даних від випадкової втрати або знищення, незаконної обробки, у тому числі незаконного знищення чи доступу до них.

Крім цього, відповідно до частини третьої статті 10 Закону, працівники володільця зобов'язані не допускати розголошення у будь-який спосіб персональних даних, які їм було довірено або які стали відомі у зв'язку з виконанням професійних чи службових або трудових обов'язків, окрім випадків, передбачених законом.

З цією метою володілець персональних даних повинен вжити розумних заходів, спрямованих на забезпечення захисту права суб'єкта на захист його персональних даних від незаконного доступу (поширення) (пункт 7 частина друга статті 8 Закону). Рівень заходів захисту, що повинні вживатися володільцем, визначається ним самостійно та залежить в основному від чутливості персональних даних, які ним обробляються.

Також слід наголосити, що у частині 6 статті 16 Закону мова йде саме про право доступу **суб'єкта персональних даних.** Отже, з метою запобігання зловживань, спрямованих на отримання конфіденційної інформації про особу (у даній справі мова йде про інформацію чутливого характеру) шляхом надсилання запиту від її імені, володільцю персональних даних при наданні запитуваної інформації необхідно вжити розумних заходів із метою встановлення особи запитувача та його права здійснювати

законне представництво (з огляду на те, що мова йде про отримання персональних даних дитини її батьками). **Характер таких заходів залежить від обставин кожної окремої справи.**

Дистанційно це можна здійснити шляхом співставлення певних ідентифікуючих ознак особи, найпоширенішою з яких у діловодстві є особистий підпис. Так як для письмової форми звернення/запиту наявність особистого (власноручного) підпису обов'язкова, для перевірки особи запитувача при запитуванні інформації про себе допускається витребування разом із запитом копії сторінки документа, який посвідчує особу, яка містить особистий підпис запитувача (наприклад, паспорт), що необхідно для здійснення верифікації (встановлення справжності підпису шляхом візуального порівняння зі зразком).

Окрім цього, з метою підтвердження права автора запиту представляти інтереси дитини видається необхідним надати також копію свідоцтва про народження, що повинно підтвердити факт батьківства.

Відтак, на думку Уповноваженого, за умови надання вказаних документів запитувана заявником інформація може бути надана.

Разом з тим державним органам, які працюють з великими об'ємами персональних даних, особливо якщо категорії даних, що обробляються, практично однакові (наприклад, у базах та реєстрах), рекомендується розробити політику захисту персональних даних, у якій викласти правила, що стандартизували б роботу із зверненнями суб'єктів, щодо надання доступу до їх персональних даних.

5.3. Право суб'єкта направити заперечення щодо обробки його персональних даних. Видалення та зміна персональних даних.

Відповідно до ст. 8 Закону, суб'єкт має також право: «6) пред'являти вмотивовану вимогу щодо зміни або знищення своїх персональних даних будь-яким володільцем та розпорядником персональних даних, якщо ці дані обробляються незаконно

чи є недостовірними; та… 11) відкликати згоду на обробку персональних даних».

Щодо права особи пред'являти вимогу про знищення її персональних даних, це право деталізується у статті 15 Закону, відповідно до якої «персональні дані видаляються або знищуються в порядку, встановленому відповідно до вимог закону. Персональні дані підлягають видаленню або знищенню у разі 1) закінчення строку зберігання даних, визначеного згодою суб'єкта персональних даних на обробку цих даних або законом або 2) припинення правовідносин між суб'єктом персональних даних та володільцем чи розпорядником, якщо інше не передбачено законом[19]. Персональні дані, зібрані з порушенням вимог цього Закону, підлягають видаленню або знищенню у встановленому законодавством порядку».

Крім цього, відповідно до частин першою та третьою статті 20 Закону «володільці чи розпорядники персональних даних зобов'язані вносити зміни до персональних даних на підставі вмотивованої письмової вимоги суб'єкта персональних даних. Зміна персональних даних, які не відповідають дійсності, проводиться невідкладно з моменту встановлення невідповідності».

Фактично вказані вище норми передбачають право особи вимагати: 1) зміни чи видалення даних, що не відповідають дійсності (п. 6 ч. 2 ст. 8 та ст. 20 Закону) та 2) видалення даних, що обробляються незаконно (п.п. 6 та 11 ч. 2 ст. 8 та ст. 15 Закону)

Щодо першого, важливим питанням у цьому випадку є поняття **вмотивованості вимоги**, від чого практично залежить те, чи буде вона задоволена. У кожному випадку володілець повинен вирішувати це питання в залежності від усіх обставин справи. Якщо мова йде, наприклад, про отримання суб'єктом рекламних повідомлень від володільця, для того, щоб виправити неточності в імені чи інших даних, суб'єкту достатньо просто вказати на неточність. Якщо ж зміна

19 А також у випадку: 3) видання відповідного припису Уповноваженого або визначених ним посадових осіб секретаріату Уповноваженого; 4) набрання законної сили рішенням суду щодо видалення або знищення персональних даних. Вказані підстави розглядатимуться в розділі, де мова йтиме про порядок здійснення контролю за додержанням законодавства про захист персональних даних.

інформації про суб'єкта матиме вагомі юридичні наслідки, володілець має право вимагати від суб'єкта підтвердження того, що персональні дані дійсно потрібно змінити.

Щодо другого, слід зазначити у цьому зв'язку, що статті 8 (п.п. 6 та 11 ч. 2 ст. 8) та 15 Закону неузгоджені між собою. Фактично поняття незаконності охоплює всі підстави видалення, передбачені статтею 15, та включає інші підстави для видалення персональних даних (наприклад, обробка без підстав, передбачених статтею 7 чи 11 Закону; обробка непропорційно великого об'єму даних та ін. буде також незаконною). Відтак, аналіз слід почати зі підстав для видалення персональних даних, передбачених статтею 15 Закону.

1. Відповідно до ст. 15 Закону персональні дані видаляються після закінчення строку, на який особа дала згоду. Також, згідно з пунктом 11 частини другої статті 8 Закону (див. вище), навіть якщо строки обробки погоджені сторонами не закінчилися, а особа відкликає згоду, такі дані все одно слід видалити. В підсумку, **особа має право вимагати видалення її персональних даних, коли строк обробки, на який вона давала згоду, закінчився або коли вона відкликає згоду на обробку персональних даних**. Після закінчення вказаного строку чи відкликання згоди, якщо у володільця немає інших підстав для обробки даних, будь-яка подальша обробка буде незаконною.

При цьому слід враховувати, що якщо згода не була єдиною підставою обробки персональних даних, то її відкликання не тягнутиме автоматичного видалення персональних даних, якщо інші підстави для обробки продовжують існувати.

Приклад
Особа уклала кредитний договір з банком. У такому випадку банк зазвичай оброблятиме персональні дані особи на таких підставах, передбачених законом:
- Згода: зазвичай банк бере в особи згоду на обробку її персональних даних для здійснення цільового маркетингу, тобто рекламування своїх товарів та послуг. Строк такої згоди, як правило, невизначений;
- Договір: на підставі положень договору банк оброблятиме персональні дані, необхідні для його виконання 1) впродовж строку виконання договору та 2) певний час після його закінчення для захисту своїх інтересів від можливих скарг (зазвичай цей строк не перевищує строку позовної давності);
- Закон: відповідно до Законів України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» та «Про банки і банківську діяльність», банк зобов'язаний ідентифікувати та верифікувати клієнта. З цією метою він має право на отримання низки необхідної з цією метою інформації та документів, які банк має право зберігати впродовж, визначеного законом, строку.
В певний момент особа може звернутися до банку та відкликати свою згоду на обробку персональних даних. Як наслідок, банк перестає надсилати їй рекламну продукцію та обробляти її дані з цією мето. Разом з тим, якщо інші підстави продовжують існувати, банк не зможе видалити персональні дані, необхідні для їх досягнення.

2. Також персональні дані підлягають видаленню, якщо закінчився визначений законом строк їх обробки. Вказана підстава є очевидною та не потребує коментарів.

Щодо такої передбаченої статтею 15 Закону підстави для видалення, як «припинення правовідносин між суб'єктом персональних даних та володільцем чи розпорядником, якщо інше не передбачено законом», то вона є доволі незрозумілою. Ймовірно законодавець мав на увазі виконання сторонами зобов'язання/договору. Однак, в більшості випадків

припинення правовідносин не обов'язково тягне за собою видалення персональних даних. Наприклад, як йшлося вище, виконання договору чи закінчення строку його дії не означає автоматичне видалення персональних даних, які інколи можуть бути необхідними для захисту своїх інтересів від скарг. Відтак, на разі потенційне застосування вказаного положення залишається невідомим і його слід видалити в разі перегляду Закону.

Щодо таких підстав як видання відповідного припису Уповноваженого або визначених ним посадових осіб секретаріату Уповноваженого та набрання законної сили рішенням суду щодо видалення або знищення персональних даних, то більш детально вони розглядатимуться у розділі щодо здійснення контролю за додержанням законодавства про захист персональних даних. Однак, очевидним є той факт, що вони також узгоджуються з положеннями статті 8 Закону.

Разом із тим персональні дані підлягають видаленню на вимогу суб'єкта, якщо вони обробляються **незаконно** (п.п. 6 та 11 ч. 2 ст. 8), тобто як що їх обробка суперечить 1) законодавству та 2) Закону.

Так, невідповідність **законодавству** передбачає, що жодним нормативно-правовим актом не передбачено право обробляти персональні дані суб'єкта.

Разом із тим навіть, якщо законодавством передбачено право обробляти персональні дані та визначено порядок такої обробки, вона повинна відповідати Закону, зокрема викладеним у ньому принципам законності (в частині щодо чіткості та передбачуваності положень законодавства), необхідності/ пропорційності, легітимної мети та ін. (див. розділ про принципи обробки персональних даних). Відтак, якщо законом, наприклад, передбачене право обробляти персональні дані суб'єкта впродовж 10-ти років, а реально для досягнення мети обробки необхідно 5 років, то після закінчення п'ятирічного строку така обробка суперечитиме Закону.

В разі, якщо суб'єкт доведе до відома державного органу, наприклад, те, що обробка його персональних даних не відповідає положенням Закону, то останньому слід розглянути можливість вжиття заходів щодо перегляду відповідного нормативно-правового акта, на якому базується така обробка

(такі заходи доцільні, коли порушення носить системний характер. Коли мова йде про одиничний випадок ймовірно слід перш за все видалити дані суб'єкта).

Разом із тим на перспективу видається доцільним конкретизувати та узгодити вказані положення статті 8 та 15 Закону, а саме роз'єднати право суб'єкта на внесення змін та видалення персональних даних у зв'язку з їх неточністю та його право на видалення даних. При цьому слід з урахуванням зазначених положень окремо визначити, за яких умов суб'єкт має право вимагати видалення персональних даних.

5.4. Право на заперечення проти обробки.

Згідно з частиною другою статті 8 Закону, суб'єкт персональних даних має право:

«5) пред'являти вмотивовану вимогу володільцю персональних даних із запереченням проти обробки своїх персональних даних;

12) знати механізм автоматичної обробки персональних даних;

13) на захист від автоматизованого рішення, яке має для нього правові наслідки».

Пункт 5 частини другої статті 8 Закону видається схожим із пунктом 6 (вмотивована вимога щодо зміни чи знищення), однак призначення у нього зовсім інше. Вказаний пункт був запозичений із Директиви, де він закріплює право особи у випадках, передбачених статтею 7 (e) та (f) Директиви (аналог пунктів 2 та 6 частини першої статті 11 Закону), заперечувати проти обробки її персональних даних на обґрунтованих законних підставах, що стосуються її особистої ситуації. Якщо такі заперечення обґрунтовані, володілець повинен припинити обробку її персональних даних.

Таким чином, якщо право на припинення обробки стосується даних, які обробляються незаконно, то у даному випадку мова йде про ситуації, коли елемент незаконності відсутній, однак **індивідуальні інтереси суб'єкта на захист його персональних даних переважають інтереси володільця щодо їх обробки**.

Ще одним вагомим моментом є право особи 1) на захист від автоматизованого рішення, яке має для неї правові наслідки

та 2) знати механізм автоматичної обробки персональних даних.

Перше є по суті правом особи, виходячи з її індивідуальних обставин, заперечувати проти прийняття такого автоматизованого рішення. Класичним прикладом автоматизованого рішення є ситуація, коли використовуючи надану особою інформацію, банк застосовує певний алгоритм, за допомогою якого автоматично здійснює оцінку її кредитоспроможності без урахування індивідуальних обставин (фактично особа розглядається як формальний набір сухих даних).

Право особи знати механізм автоматичної обробки даних є запорукою дотримання права на захист від автоматизованого рішення та передбачає, що особа повинна бути попереджена/повідомлена про такий механізм автоматизованої обробки.

«Механізм автоматичної обробки» традиційно називається профайлингом. Згідно з Регламентом профайлингом є «будь-яка автоматизована обробка персональних даних, яка полягає у використанні персональних даних для того, щоб оцінити певні особисті аспекти фізичної особи, зокрема, проаналізувати чи спрогнозувати працездатність особи, фінансову ситуацію, стан здоров'я, споживацькі вподобання, інтереси, надійність, поведінку, місцезнаходження чи шляхи пересування».

Фактично це явище з точки зору законодавства про захист персональних даних має два негативні елементи:

1) аналізуючи отриману щодо особи інформацію (яку вона, наприклад, надає за згодою чи на підставі договору), володілець створює новий масив даних про особу, дозволу на обробку яких він не має і який зазвичай носить більш чутливий характер. Так, тривалий час купуючи товари у супермаркеті за допомогою отриманої картки покупця суб'єкт передає володільцю інформацію щодо здійснених ним покупок. Проаналізувавши таку інформацію (за допомогою певного алгоритму (механізму) автоматизованої обробки), володілець отримує додаткову інформацію щодо споживацьких вподобань, майнового стану та певних особистих звичок (наприклад, час та день здійснення закупів). Незалежно від подальшого використання такі дії є суттєвим втручання в права особи,

гарантовані Законом;

2) отримавши додаткову інформацію, володілець може використовувати її шляхом, що матиме наслідки для суб'єкта (див. вище приклад щодо оцінки кредитоспроможності). Так, наприклад суб'єкт отримуватиме рекламу товарів, що відповідають його купівельній спроможності, чи товарів, що можуть його зацікавити.

Таким чином, з огляду на те, що такі дії мають наслідком створення нової інформації щодо особи (її персональних даних), володілець повинен мати відповідні підстави для її обробки. Відтак, до здійснення володільцем профайлингу повинні застосовуватися ті ж положення Закону, що і до решти даних, а саме: він повинен здійснюватися за згодою особи або на підставі закону, відповідати підставам законної обробки (див. стаття 7 та 11 Закону), відповідати принципам обробки персональних даних, доводитися, як це передбачено статтею 8 Закону до відома особи, щодо якої застосовуватиметься та ін..

Крім цього, як вже зазначалося вище, навіть якщо профайлинг законно застосовується, особа повинна мати можливість заперечити проти застосування у її ситуації його результатів.

5.5. Інші права.

Відповідно до частини другої статті 8 Закону суб'єкт має право:

1) 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;

2) звертатися із скаргами щодо обробки своїх персональних даних;

3) застосовувати засоби правового захисту в разі порушення законодавства про захист персональних даних. Ці положення буде більш детально розглянуто нижче.

Виходячи з цих норм, а також прав, що розглядалися вище, суб'єкт має як мінімум такі засоби захисту: звернення зі скаргою до володільця, Уповноваженого та суду.

Видається логічним, щоб свою першу скаргу суб'єкт направляв до володільця. Це може бути необов'язково власне скарга, а заперечення проти обробки чи вимога щодо припинення незаконної обробки. В разі отримання відмови, яка, на думку суб'єкта, є необґрунтованою він може звернутися до Уповноваженого чи суду. У такому випадку його скарга до Уповноваженого буде більш обґрунтованою та переконливою (оскільки міститиме відповіді володільця). Окрім цього, в такому випадку Уповноважений не потребуватиме додаткових документів, отримання яких займає більше часу, та за певних умов зможе відразу вжити необхідних заходів реагування.

Слід лише зазначити, що право застосовувати засоби правового захисту та звертатися зі скаргою передбачає не лише гарантії незалежного та безстороннього розгляду скарги та прийняття рішення, здатного виправити порушення прав суб'єкта в разі, якщо воно мало місце, а й імпліцитно гарантує особі можливості мати достатні ресурси для захисту своїх прав, тобто документи та інформацію, що мають значення для вирішення його справи. Це передбачає **обов'язок володільця детально фіксувати та документувати свою діяльність щодо обробки персональних даних** (див. також вище розділ щодо отримання суб'єктом даних щодо третіх осіб, яким передавалися персональні дані). Саме володілець повинен у разі направлення суб'єктом скарги мати можливість довести, що ним не було вчинено порушення, та надати відповідні докази. У зазначених вище гарантіях не було би жодного сенсу, якби володілець міг не зберігати інформацію щодо обробки персональних даних (чи безслідно знищити її) та в разі отримання скарги посилатися на неможливість доведення його причетності/вини в порушенні законодавства про захист персональних даних. Якщо володілець не може надати документи, що прямо заперечують його причетність до порушення прав суб'єкта чи демонструють, що він вжив всіх заходів, необхідних для запобігання вчиненню такого правопорушення, він повинен нести за це відповідальність.

5.6. Висновки.

Зазначені вище права є пов'язаними та лише комплексне їх дотримання гарантує суб'єкту можливість контролювати

обробку його персональних даних. Недотримання одних прав автоматично тягне за собою порушення інших.

1. Суб'єкта повинні автоматично інформувати про обробку його персональних даних, підстави та мету, порядок та механізми такої обробки.

2. Виходячи із отриманої інформації, він може самостійно звернутися до володільця та отримати більш детальну інформацію про обробку персональних даних

3. Отримавши весь спектр інформації щодо обробки його персональних даних, суб'єкт може оцінити законність їх обробки та: 1) вимагати їх видалення, 2) вимагати їх зміни, 3) звертатися зі скаргою до суду чи Уповноваженого.

6. ОБМЕЖЕННЯ ДІЇ ПРАВ СУБ'ЄКТА ПЕРСОНАЛЬНИХ ДАНИХ.

Як вже йшлося вище у розділах щодо підстав обробки чутливих категорій персональних даних та права суб'єкта на отримання інформації щодо обробки його персональних даних реалізація усіх вказаних вище прав суб'єкта персональних даних та принципів обробки може обмежуватися на підставі статті 25 Закону. **Згідно з частиною 1 статті 25 Закону** обмеження дії статей 6 (принципи обробки), 7 (обробка чутливих категорій персональних даних) і 8 (права суб'єкта персональних даних) Закону може здійснюватися у випадках, передбачених законом, наскільки це необхідно у демократичному суспільстві в інтересах національної безпеки, економічного добробуту або захисту прав і свобод суб'єктів персональних даних чи інших осіб.

Відтак, обмеження дії вказаних статей можливе лише, якщо: 1) передбачене законом; 2) необхідне/пропорційне; 3) переслідує одну з легітимних цілей – національної безпеки, економічного добробуту або захисту прав і свобод суб'єктів персональних даних чи інших осіб.

Виникає цікава ситуація: виходить, що обмеження до принципів законності, легітимної мети та необхідності повинні бути законними, необхідними та переслідувати легітимну мету.

Вказане вище свідчить про те, що фактично **не може бути жодних обмежень до принципів легітимної**

мети, необхідності та законності. Вказані принципи є зобов'язаннями володільця, що повинні дотримуватися ним за будь-яких умов.

Разом із тим, не виникає жодних сумнівів, що за умови дотримання положень статті 25 Закону можна обмежити застосовність принципу прозорості, відкритості, прав суб'єкта персональних даних, а також відступити від положень статті 7 Закону. Так, якщо це **необхідно**, **визначено законом** та **переслідує одну з цілей, передбачених статтею 25 Закону**, можна обмежити, наприклад, доступ суб'єкта до своїх персональних даних.

Приклад.
Відповідно до частини першої статті 39 «Основ законодавства України про охорону здоров'я» за загальним правилом пацієнт, який досяг повноліття, має право на отримання достовірної і повної інформації про стан свого здоров'я, у тому числі на ознайомлення з відповідними медичними документами, що стосуються його здоров'я (частина перша статті 39).
Разом із тим, відповідно до ч. 4 ст. 39, якщо інформація про хворобу пацієнта може погіршити стан його здоров'я або погіршити стан здоров'я фізичних осіб, визначених частиною другою цієї статті, зашкодити процесові лікування, медичні працівники мають право надати неповну інформацію про стан здоров'я пацієнта, обмежити можливість їх ознайомлення з окремими медичними документами.
Цим положенням закону (частиною 4) обмежується право особи на ознайомлення з інформацією про себе. Однак, таке обмеження встановлене законом (частина 4 статті 39), переслідує легітимну мету (захист прав пацієнта або інших осіб) та є необхідним для її досягнення (в іншому випадку (мається на увазі в разі надання інформації) може бути завдана шкода здоров'ю пацієнта/інших осіб, виникнуть перешкоди належному лікуванню).

Див. також приклад з практики роботи Уповноваженого

ВРУ з прав людини вище.

Щодо **обмеження державним органом доступу суб'єкта до своїх персональних даних**, то тут слід зважувати одночасно положення декількох законів.

Перш за все, згідно з статтею 32 Конституції України «Кожний громадянин має право знайомитися в органах державної влади, органах місцевого самоврядування, установах і організаціях з відомостями про себе, які не є **державною або іншою захищеною законом таємницею**».

Згідно зі ст. 8 Закону України «Про доступ до публічної інформації» «таємна інформація – це інформація, доступ до якої обмежується **відповідно до частини другої статті 6 цього Закону та** розголошення якої може завдати шкоди особі, суспільству і державі».

Згідно з частиною другою статті 6 Закону «Про доступ до публічної інформації» обмеження доступу до інформації здійснюється відповідно до закону при дотриманні сукупності таких вимог:

1) виключно в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя;

2) розголошення інформації може завдати істотної шкоди цим інтересам;

3) шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні.

Звідси випливає, що доступ особи до інформації про себе обмежується лише на **підставі закону** (стаття 6 та 8 Закону України «Про доступ до публічної інформації»), **в цілях та на умовах, передбачених пунктом 1 частини другої статті 6 вказаного Закону**. Вказані цілі повністю відповідають тими, що передбачені статтею 25 Закону (хоч перелік цілей дещо і відрізняється). Пункти 2 та 3 частини другої статті 6 Закону України «Про доступ до публічної інформації» є більш

деталізованим варіантом принципу необхідності, про який мова йде у статті 25 Закону.

Відтак, кожного разу, обмежуючи доступ суб'єкта до його персональних даних, державний орган повинен продемонструвати, що таке обмеження є законним, переслідує легітимну мету та є необхідним у кожному конкретному випадку.

7. ПОРЯДОК ОРГАНІЗАЦІЇ ВОЛОДІЛЬЦЕМ ПРОЦЕСУ ОБРОБКИ ТА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ.

7.1.Основні складові організації процесу обробки та захисту персональних даних.

Поняття захисту персональних даних є доволі широким та зазвичай включає два ключових елемента.

По-перше, це **зобов'язання володільця** вживати організаційних та технічних заходів з метою запобігання їх випадкової втрати або знищення, незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних (стаття 24 Закону).

По-друге, це **зобов'язання кожного працівника** володільця та розпорядника не допускати розголошення персональних даних, які стали йому відомі у зв'язку з виконанням професійних чи службових або трудових обов'язків, так зване зобов'язання конфіденційності (стаття 10 Закону).

Володілець персональних даних самостійно повинен визначати, яких заходів слід вживати з метою забезпечення захисту персональних даних. В будь-якому такі заходи повинні бути пропорційними потенційним ризикам, пов'язаним з обробкою персональних даних, які здійснює володілець. Перелік обов'язкових заходів захисту, які повинні вживатися всіма володільцями, визначено Типовим порядком обробки персональних даних, затвердженим наказом Уповноваженого від 08.01.2014 № 1/02-14. Ці вимоги носять загальний характер і є мінімальними вимогами у сфері захисту персональних

даних, а шляхи їх практичної імплементації вирішуються в індивідуальному порядку кожним окремим володільцем.

3.4. Організаційні заходи охоплюють:
- визначення порядку доступу до персональних даних працівників володільця/розпорядника;
- визначення порядку ведення обліку операцій, пов'язаних з обробкою персональних даних суб'єкта та доступом до них;
- розробку плану дій на випадок несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, виникнення надзвичайних ситуацій;
- регулярне навчання співробітників, які працюють з персональними даними.

3.5. Володілець/розпорядник веде облік працівників, які мають доступ до персональних даних суб'єктів. Володілець/розпорядник визначає рівень доступу зазначених працівників до персональних даних суб'єктів. Кожен із цих працівників користується доступом лише до тих персональних даних (їх частини) суб'єктів, які необхідні йому у зв'язку з виконанням своїх професійних чи службових або трудових обов'язків.

3.6. Усі інші працівники володільця/розпорядника мають право на повну інформацію лише стосовно власних персональних даних.

3.7. Працівники, які мають доступ до персональних даних, дають письмове зобов'язання про нерозголошення персональних даних, які їм було довірено або які стали їм відомі у зв'язку з виконанням професійних чи службових або трудових обов'язків.

3.8. Датою надання права доступу до персональних даних вважається дата надання зобов'язання відповідним працівником.

3.9. Датою позбавлення права доступу до персональних даних вважається дата звільнення працівника, дата переведення на посаду, виконання обов'язків на якій не пов'язане з обробкою персональних даних.

3.10. У разі звільнення працівника, який мав доступ до персональних даних, або переведення його на іншу посаду, що не передбачає роботу з персональними даними суб'єктів,

вживаються заходи щодо унеможливлення доступу такої особи до персональних даних, а документи та інші носії, що містять персональні дані суб'єктів, передаються іншому працівнику.
(…)
3.14. З метою забезпечення безпеки обробки персональних даних вживаються спеціальні технічні заходи захисту, у тому числі щодо виключення несанкціонованого доступу до персональних даних, що обробляються та роботі технічного та програмного комплексу, за допомогою якого здійснюється обробка персональних даних.
(…)

Таким чином, перш за все володілець повинен забезпечити, щоб до персональних даних мали доступ лише ті працівники, які з ними працюють. Кожному з таких працівників повинен надаватися доступ до тих даних, які йому необхідні у зв'язку з виконанням його службових обов'язків. Окрім цього, володілець повинен зберігати інформацію/документи щодо того, які працівники та впродовж якого часу мали доступ до тих чи інших персональних даних. Такі заходи необхідні для того, щоб у разі поширення, втрати, знищення персональних даних звузити коло осіб, що можуть бути до цього причетними. Для цього, володільцю (в залежності від масштабу діяльності, кількості працівників володільця) доцільно визначити типові рівні доступу.

Приклад.
Підприємство веде базу даних, в яку включаються такі дані клієнтів:
1) прізвище, ім'я та по батькові, 2) рік, дата народження та вік, 3) телефон/електронна адреса, 5) адреса проживання, 6) місце роботи (сфера зайнятості), 7) дані про склад сім'ї, 8) дані про придбані товари.
Доступ до бази даних передбачається надавати на 4-х рівнях:
Керівник – доступ до всіх категорій даних;
Спеціаліст-маркетолог (розробка та реалізація заходів щодо просування товарів володільця на ринку) – доступ до 2, 3, 6, 7, 8;
Спеціаліст із закупівель – 8;
Спеціаліст з продажу (прийняття замовлення та доставка товару) – доступ до 1, 2, 3 категорії даних;
Спеціаліст по роботі з постійними клієнтами – доступ до 1-8 категорії даних.
Відтак, якщо ретельно розмежовувати рівні доступу, з персональними даними працюватиме лише невелика кількість працівників.

Перед отриманням доступу до персональних даних кожен працівник повинен пройти процедуру ідентифікації/автентифікації, зокрема шляхом особистого введення індивідуального та відомого лише йому паролю (чи іншим способом, наприклад шляхом використання індивідуальної картки, яка автоматичну запускає визначені для конкретного користувача налаштування та ін.). Це повинно забезпечити, що лише визначений працівник зможе працювати за певним робочим місцем чи за будь-яким робочим місцем, однак із визначеними особисто для нього налаштуваннями доступу до персональних даних. Окрім цього, це дасть змогу ідентифікувати працівників, які працюють в системі, за допомогою присвоєного ними ідентифікатора.

Володілець може здійснювати контроль доступу до приміщень, де зберігаються картотеки/сервери з персональними даними, та робочих приміщень загалом. Залежно від важливості

інформації, що зберігається в базі даних, приміщення можуть обладнуватися автоматичними електронними замками, сигналізацією тощо. В якості додаткового заходу безпеки володільці можуть (з дотриманням певних гарантій) із метою контролю за виробничою дисципліною, дотриманням правил трудової етики здійснювати нагляд за працівниками.

Якщо володільцем здійснюється автоматизована обробка персональних даних, рекомендується вжити заходів щодо створення резервної копії інформації, антивірусного захисту, захисту каналів передачі інформації (криптографічного, фізичного) від несанкціонованого втручання.

Крім цього, в разі якщо володілець обробляє великі масиви даних і до цього процесу залучена велика кількість працівників для того, щоб стандартизувати роботу, програмне забезпечення, яке використовується для обробки персональних даних, має бути розроблене таким чином, щоб позбавити працівників можливості вводити зайві об'єми персональних даних та проводити недопустимі операції з обробки (наприклад, несанкціоноване копіювання, друк та інше) або ж контролювати такі процеси. Саме програмне забезпечення повинне по можливості приймати рішення щодо строків збереження інформації та в разі їх закінчення автоматично її видаляти.

Вказані вимоги відповідають правилу захисту персональних даних за умовчанням (*privacy by default*), який станом на сьогодні вже пройшов процес становлення серед держав-членів Європейського Союзу. Так, стаття 25 Регламенту передбачає, що володілець зобов'язаний впроваджувати механізми гарантування того, що за замовчуванням обробляються лише ті персональні дані, які є необхідними для кожної детально визначеної мети обробки, і не зберігаються поза межами мінімальних строків, необхідних для досягнення таких цілей. Ці механізми повинні також забезпечити, щоб персональні дані не були доступними невизначеному колу осіб.

Володілець повинен забезпечити і регулярне навчання своїх співробітників, їх ознайомлення з порядком обробки персональних даних та отримати від них зобов'язання щодо конфіденційності інформації.

Більшої конкретики в частині, що стосується методу визначення відповідності заходів захисту, ні Закон, ні інші нормативно-правові акти у сфері захисту персональних даних не надають. Законодавство у сфері безпеки інформації, зокрема Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», Постанова КМУ від 29 березня 2006 року № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» та передбачені ними нормативно-правові акти, встановлює більш детальні вимоги щодо технічного захисту інформації, які, все ж слід зазначити, є доволі жорсткими та не враховують особливостей того чи іншого володільця (зокрема, його фінансових можливостей, масштабів обробки персональних даних, характеру даних).

Крім цього, як зазначалося вище, саме володілець повинен **мати змогу продемонструвати дотримання законодавства про захист персональних даних** (див. розділ про права суб'єкта персональних даних).

Так, суб'єкт за загальними правилом має право отримувати інформацію щодо джерел отримання його персональних даних володільцем, складу та змісту даних, а також інформацію про те, кому вони передавалися (частина друга статті 8 Закону). Володілець, своєю чергою, повинен забезпечити можливість отримання цієї інформації та можливість її матеріального підтвердження (документами, витягами з роботи програмного забезпечення автоматизованих систем обробки персональних даних, у вигляді звітів, електронних журналів обліку або аудиту, витягів з автоматизованих систем тощо).

Вказане зобов'язання володільця випливає також із права суб'єкта на доступ до засобів захисту в частині порушення його прав на захист персональних даних (і в тому числі, права направити скаргу до Уповноваженого чи суду), а також компетенції Уповноваженого (частина друга статті 8 та стаття 23 Закону). Так, право особи на захист своїх прав не матиме сенсу у випадку, якщо неможливо буде встановити ким, коли, у який спосіб оброблялися та кому передавалися його персональні дані.

Правильність саме такого тлумачення норм чинного законодавства підтверджується тим, як тлумачаться аналогічні норми Директиви судовими інституціями Європейського Союзу (див. вище у розділі про права суб'єкта персональних даних рішення Суду справедливості ЄС у справі У справі «Мер і члени міської ради Роттердаму проти М.Е.Е. Ріджкебура»[20]).

Вказане зобов'язання передбачено Регламентом у частині 2 статті 5 та статті 30.

У зв'язку з цим та на виконання вказаних вище положень Закону Уповноваженим в пункті 3.11 Типового порядку обробки персональних даних було передбачено обов'язок володільця здійснювати **облік операцій, пов'язаних з обробкою персональних даних суб'єкта та доступом до них працівників**.

Типовий порядок обробки персональних даних
(…)
3.11. Володілець/розпорядник веде облік операцій, пов'язаних з обробкою персональних даних суб'єкта та доступом до них. З цією метою володільцем/розпорядником зберігається інформація про:
- дату, час та джерело збирання персональних даних суб'єкта;
- зміну персональних даних;
- перегляд персональних даних;
- будь-яку передачу (копіювання) персональних даних суб'єкта;
- дату та час видалення або знищення персональних даних;
- працівника, який здійснив одну із указаних операцій;
- мету та підстави зміни, перегляду, передачі та видалення або знищення персональних даних.
Володілець/розпорядник персональних даних самостійно визначає процедуру збереження інформації про операції, пов'язані з обробкою персональних даних суб'єкта та доступом до них. У випадку обробки персональних даних суб'єктів за допомогою автоматизованої системи така система автоматично фіксує вказану інформацію.

20 CJEU, C-553/07, College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer, 7 May 2009.

Ця інформація зберігається володільцем/розпорядником упродовж одного року з моменту закінчення року, в якому було здійснено зазначені операції, якщо інше не передбачено законодавством України.
(…)

Недотримання вказаного зобов'язання становитиме серйозне порушення прав суб'єкта персональних даних.

Приклад 1. Справа «I. v. Finland»[21]

До Європейського суду звернулася особа, що була хворою на СНІД. Вона проходила лікування у лікарні, де вона і працювала. В певний момент інформація про діагно заявниці стала відомою широкому колу працівників лікарні. Вона, звернулася за захистом своїх прав до суду. Їй було відмовлено в задоволенні скарг. Суди визнали, що інформацію було незаконно поширено кимось з працівників лікарні. Однак інформація щодо того, хто міг це зробити, зокрема, хто переглядав дані заявниці, не зберігалася лікарнею. До Суду заявниця звернулася зі скаргою на неспроможність лікарні гарантувати захист її даних від несанкціонованого доступу.

Розглянувши матеріали справи, Суд встановив, що «заявниця програла цивільну справу через те, що не змогла довести причинно-наслідкового зв'язку між недоліками в правилах доступу та поширенням інформації про стан її здоров'я. Цілком очевидно, що якби лікарня забезпечила сильніший контроль над доступом до медичних карток, обмеживши доступ до них лише для медперсоналу, який безпосередньо був задіяний у лікуванні заявниці, або запровадила ведення обліку всіх осіб, які мали доступ до медичної картки заявниці, остання мала би більш вигідні позиції під час проваджень у національних судах. На думку Суду, вирішальним є той факт, що система ведення документації в лікарні справді не відповідала нормативно-правовим вимогам, визначеним статтею 26 Закону «Про особисті дані» (відповідно до якої особа, яка працює з персональними даними, повинна переконатися, що

21 I. v. Finland, no. 20511/03, 17 July 2008

персональні дані й інформація, яка перебуває в оброблюваних записах, відповідним чином захищена від незаконної обробки, використання, знищення, зміни або викрадення), і саме цьому факту національні суди не приділили належної уваги». Суд дійшов висновку, що було порушено статтю 8.

Приклад 2. Практика Уповноваженого ВРУ з прав людини.

У 2015 році до Уповноваженого звернулася заявниця зі скаргою про те, що співробітниками лікарні їй було повідомлено про те, що її медична картка зникла з поліклініки.

У зв'язку зі зазначеною скаргою Уповноваженим було відкрито провадження, в рамках якого направлено вимогу про надання коментарів щодо скарги заявниці керівником поліклініки. Крім цього, Уповноваженим було запитано інформацію щодо того, чи зберігається/лася в поліклініці медична картка заявниці, і якщо так, то кому та коли вона востаннє передавалася. Вказану інформацію слід було підтвердити відповідними документами.

Лікарня повідомила, що медична картка є в самої заявниці.

Уповноваженим було досліджено матеріали справи (скаргу заявниці, коментарі керівника поліклініки, наявну облікову медичну документацію, журнали вхідної кореспонденції, журнал видання та повернення амбулаторних карток тощо) та встановлено, що із наявних матеріалів немає можливості встановити, де медична картка та хто причетний до її зникнення.

Так, в журналі видання та повернення амбулаторних карток міститься інформація щодо видачі та повернення медичних карток пацієнтів (лікарями та пацієнтами). У ньому не було відомостей щодо картки заявниці. Разом з тим, в лікарні відсутній загальний опис медичної документації, що є в її володінні.

У зв'язку з цим Уповноваженим було констатовано порушення таких положень законодавства:

− пунктів 1, 2 та 4 частини другої статті 8 Закону:

«Суб'єкт персональних даних має право: 1) знати про (…) місцезнаходження своїх персональних даних (…);

2) отримувати інформацію про (…) третіх осіб, яким передаються його персональні дані; 4) отримувати не пізніш як за тридцять календарних днів з дня надходження запиту, крім випадків, передбачених законом, відповідь про те, чи обробляються його персональні дані, а також отримувати зміст таких персональних даних».

Вказані положення, на думку Уповноваженого, вимагають від володільців бути готовими надати (крім випадків, визначених законом) суб'єкту чи Уповноваженому вичерпну інформацію щодо того, чи обробляються ним персональні дані суб'єкта, а також, коли та кому вони передавалися.

частини першої статті 24 Закону:

«Володільці, розпорядники персональних даних та треті особи зобов'язані забезпечити захист цих даних від випадкових втрати або знищення, від незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних».

На думку Уповноваженого, очевидно, що володілець не зможе в достатній мірі захистити персональні дані суб'єктів від незаконних дій, якщо він не володіє інформацією щодо того, якими даними він володіє та хто має до них доступ.

- п. 3.11 Типового порядку обробки персональних даних, затвердженого наказом Уповноваженого від 8 січня 2014 року № 1/02-14 згідно з яким володілець зобов'язаний вести «облік операцій, пов'язаних з обробкою персональних даних суб'єкта та доступом до них».

З огляду на зазначене вище, Уповноваженим було внесено поліклініці припис про усунення виявлених правопорушень, а саме: **проведення опису всієї наявної в розпорядженні поліклініки медичної документації, зокрема, за іменем суб'єкта персональних даних.**

7.2. Статус осіб та структурних підрозділів, відповідальних за захист персональних даних.

Відповідно до ч. 2 ст. 24 Закону, **в органах державної**

влади, органах місцевого самоврядування, (…) створюється (визначається) структурний підрозділ або відповідальна особа, що організовує роботу, пов'язану зі захистом персональних даних при їх обробці. Основне завдання такої посадової особи полягає у тому, щоб налагодити належним чином роботу з персональними даними, що обробляються володільцем / розпорядником чи вжити всіх можливих заходів з метою налагодження такої роботи (оскільки останнє слово все ж заливається за керівництвом володільця - розпорядника).

Компетенція та повноваження такої особи чи підрозділу зазвичай самостійно визначаються володільцем у його внутрішніх документах. Законодавство надає лише їх мінімальний перелік.

Відповідно до ч. 3 ст. 24 Закону, структурний підрозділ або відповідальна особа, що організовує роботу, пов'язану зі захистом персональних даних при їх обробці:

1) інформує та консультує володільця або розпорядника персональних даних з питань додержання законодавства про захист персональних даних;

2) взаємодіє з Уповноваженим Верховної Ради України з прав людини та визначеними ним посадовими особами його секретаріату з питань запобігання та усунення порушень законодавства про захист персональних даних.

З метою реалізації вказаних завдань відповідальна особа повинна володіти відповідними повноваженнями, мінімальний перелік яких визначено у Типовому порядку обробки персональних даних, затвердженому наказом Уповноваженого від 8 січня 2014 року № 1/02-14.

Так, відповідальна особа:

1) користується доступом до будь-яких даних, які обробляються володільцем /розпорядником та до всіх приміщень володільця/розпорядника, де здійснюється така обробка;

2) у разі виявлення порушень законодавства про захист персональних даних повідомляє про це керівника володільця/ розпорядника з метою вжиття необхідних заходів та ін.

Нижче подано розширений перелік типових функцій та повноважень структурного підрозділу/відповідальної особи, які повинні забезпечити належне виконання покладених на

них завдань.

Загалом володілець вправі самостійно визначати функції та повноваження такої особи/підрозділу в залежності від операцій з обробки, що здійснюються володільцем. Зазвичай такі функції передбачають необхідність:

1) проводити оцінку ризиків від обробки персональних даних володільцем та надавати з урахуванням проведеної оцінки консультації володільцю щодо належної організації процесу обробки персональних даних (та документувати цю діяльність);

- З цією метою відповідальна особа/підрозділ перш за все повинна, виходячи з того, яка мета обробки персональних даних володільцем, склад персональних даних, категорії суб'єктів персональних даних та операції з обробки, які здійснюються (планується здійснювати) володільцем, оцінити потенційні ризики від таких операцій з обробки. Зокрема, наскільки суттєвою буде шкода, завдана суб'єкту від втрати (видалення) таких даних, їх незаконного чи випадкового поширення, а також наскільки сильна мотивація у працівників володільця, третіх осіб намагатися отримати ці дані чи незаконно комусь передати. Виходячи з проведеної оцінки, відповідальна особа чи структурний підрозділ розробляє пропозиції щодо порядку захисту персональних даних, роботи із запитами суб'єктів та третіх осіб, визначення оптимального складу даних, що підлягатиме обробці, порядок збору персональних даних та повідомлення про це суб'єкта, порядку та рівнів доступу працівників до персональних даних, порядок документування процесів, пов'язаних з обробкою персональних даних та ін. З цією метою у державних органах така відповідальна особа повинна бути залучена до усіх процесів, пов'язаних з розробкою нормативно правових актів, що регламентуватимуть порядок обробки персональних даних володільцем.

2) консультувати в разі необхідності від інші підрозділи володільця щодо розгляду запитів суб'єктів та третіх осіб про отримання доступу до персональних даних;

3)проводити моніторинг процесів обробки персональних даних на предмет їх відповідності законодавству та Закону. Так, відповідальна особа/

підрозділ може здійснювати аудит дотриманням володільцем чи розпорядником законодавства про захист персональних даних. В разі виявлення порушень, а саме недотримання законодавства чи недоліків у самому законодавстві, доводити результати роботи до відома керівництва з рекомендаціями щодо усунення вказаних проблем.

4) у разі виявлення порушення прав суб'єктів персональних даних, відразу доводити це до відома керівництва та Уповноваженого, надавати рекомендації керівництву щодо вжиття першочергових заходів, спрямованих на мінімізацію потенційних негативних наслідків, ініціювання розслідування інциденту, повідомлення суб'єкта/ів персональних даних, чиї права порушено.

5) ознайомлювати керівництво та працівників володільця із вимогами чинного законодавства про захист персональних даних, змінами до законодавства, актуальними питання обробки персональних даних у сфері діяльності володільця, організовувати відповідні навчання для працівників;

6) взаємодіяти з Уповноваженим, що може появлятися у таких основних напрямках: 1) консультації з приводу доцільності та порядку обробки персональних даних володільцем, отримання з цього приводу роз'яснень Уповноваженого; 2) направляти Уповноваженому для погодження розроблені проекти нормативно-правових актів, що стосуються питань обробки персональних даних); 3) співпрацювати в ході проведення Уповноваженим перевірки володільця (забезпечення швидкого надання усієї інформації щодо обробки персональних даних володільцем, супровід в ході проведення перевірки, забезпечення вільного доступу до усіх приміщень, де здійснюється обробка персональних даних, та безпосередньо до інформації (і в тому числі персональних даних), що обробляється володільцем та інше); 4) забезпечення вчасного та повного виконання приписів Уповноваженого.

З метою виконання таких функцій відповідальна особа/ підрозділ повинна володіти відповідними повноваженнями, а саме:

1) безперешкодного доступу до приміщень, де здійснюється обробка персональних даних;

2) доступу до всієї інформації та документів, що стосуються здійснення володільцем чи розпорядником обробки персональних даних, і в тому числі персональних даних, що містяться у базах даних володільця, журналу реєстрації обліку операцій, пов'язаних із обробкою персональних даних та інші;

3) завчасно отримувати повну інформацію щодо будь-яких операцій, пов'язаних з обробкою персональних даних, що плануються володільцем/розпорядником;

4) право безпосереднього звітування керівництву володільця чи розпорядника.

Крім цього, для виконання вказаних вище завдань та функцій відповідальна особа/підрозділ повинні володіти відповідними навиками та статусом. Так, це повинна бути особа, яка володіє відповідною кваліфікацією у сфері захисту персональних даних та безпеки інформації. Для цього рекомендується наявність у неї відповідної освіти чи проходження такою особою відповідного спеціалізованого навчання.

Законодавство / внутрішньовідомчі документи та посадова інструкція цієї особи/положення про підрозділ повинні гарантувати незалежність та безсторонність такої особи. Для цього рекомендується, щоб обов'язки щодо організації процедури захисту персональних даних було покладено на особу, що належить до керівного складу володільця (чи підпорядковується безпосередньо керівництву). Якщо на відповідальну особу покладено також інші обов'язки, вони не повинні конфліктувати з її обов'язками щодо організації роботи, пов'язаної зі захистом персональних даних. Крім цього, таку особу має бути забезпечено всім необхідним (зокрема фінансовими та людськими ресурсами) для ефективного виконання нею своїх обов'язків. Керівники володільця не мають права примушувати відповідальних осіб до надання тих чи інших рекомендацій чи виконання певним чином їх обов'язків у сфері захисту персональних даних.

7.3. Порядок організації володільцем процесу обробки персональних даних

Державними органами влади обробка персональних даних здійснюється в основному якщо вона необхідна для виконання завдань такого органу, покладених на нього обов'язків та належної організації власної роботи. Будь-яка обробка персональних даних державним органом повинна бути законною.

Згідно з принципом законності 1) здійснення обробки персональних даних повинно базуватися на положеннях закону; 2) порядок обробки повинен регламентуватися законодавством.

Виходячи із Закону та Типового порядку обробки персональних даних, документи, що регламентують обробку персональних даних повинні **якомога чіткіше визначати**:

1) інформація про володільця персональних даних. Якщо їх декілька – інформація про кожного, а також співвідношенні їх повноважень;
2) інформація про розпорядника персональних даних (в разі наявності);
3) мету обробки персональних даних (див. більш детально вимоги щодо формулювання мети у параграфі 3.2.);
4) категорії суб'єктів, чиї персональні дані обробляються;
5) склад персональних даних, що обробляються;
6) порядок та спосіб збору персональних даних;
7) порядок верифікації та видалення персональних даних;
8) строк зберігання персональних даних;
9) гарантії дотримання прав суб'єктів персональних даних:

   - порядок реалізації права суб'єкта на доступ до своїх персональних даних;
   - порядок надання інформації щодо порядку обробки персональних даних;
   - порядок надання інформації щодо того, яким третім особам передавалися дані;
   - порядок розгляду звернень щодо видалення чи зміни персональних даних;
   - порядок розгляду заперечень проти обробки персональних даних;

- порядок розгляду скарг на незаконність обробки персональних даних;

10) треті особи, яким передаються / яким надається доступ до персональних даних;
11) здійснення транскордонної передачі даних (в разі наявності): підстави, порядок та отримувачі;
12) технічні та організаційні засоби захисту персональних даних (нижче наводиться приблизний перелік):
    - розмежування рівнів доступу працівників володільця до персональних даних та їх повноважень щодо обробки;
    - порядок та умови отримання працівниками доступу до персональних даних;
    - ведення обліку операцій обробки персональних даних (фіксація в журналі відомостей щодо особи, яка здійснює операцію, характер дій щодо персональних даних (перегляд, копіювання, друк, передача та ін.), щодо яких персональних даних, час таких дій та ін.);
    - псевдонімізація та криптографічний захист персональних даних;
    - тестування та оновлення системи технічного захисту;
    - інше.
13) алгоритм дій на випадок випадкової втрати чи зміни персональних даних, їх незаконної обробки;

Слід також зазначити, що усі зазначені елементи процесу обробки персональних даних необхідно визначити до початку обробки. У пояснювальній документації до проекту нормативно-правового акту потрібно, в разі необхідності, надати оцінку потенційних ризиків, пов'язаних із пропонованою обробкою персональних даних, необхідність обробки саме визначеного складу персональних даних та здійснення тих чи інших процедур обробки, достатність передбаченого рівня технічного та організаційного захисту персональних даних, обґрунтованість обмеження реалізації прав суб'єктів персональних даних, гарантії дотримання Закону та висновок Уповноваженого ВРУ з прав людини щодо запропонованої обробки.

Слід також зазначити, що незалежно від того наскільки детально регламентується порядок обробки тих, чи інших

персональних даних державним органами (їх територіальним підрозділам) рекомендується прийняти політику захисту персональних даних. У такому документі необхідно визначити завдання, функції та повноваження особи чи структурного підрозділу відповідального за організацію процесу обробки персональних даних, обов'язки працівників щодо захисту персональних даних, порядок роботи із запитами щодо доступу до персональних даних та зверненнями громадян (що завжди містять персональні дані особи), порядок доступу до приміщень та систем, де здійснюється обробка персональних даних та ін. Такий документ повинен врегульовувати ті питання, що не охоплюються нормативно-правовими актами, а також деталізувати їх положення та пристосовувати до реалій роботи відповідного державного органу (його структурного територіального підрозділу).

8. ПОРЯДОК ЗДІЙСНЕННЯ КОНТРОЛЮ ЗА ДОДЕРЖАННЯМ ЗАКОНОДАВСТВА ПРО ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ

1 січня 2014 року набрали чинності зміни до Закону, відповідно яких повноваження щодо здійснення контролю за додержанням законодавства про захист персональних даних було передано Уповноваженому ВРУ з прав людини. У зв'язку з цим з метою реалізації вказаних повноважень Уповноваженим було запроваджено посаду представника Уповноваженого з питань захисту персональних даних, а в структурі Секретаріату Уповноваженого створено Департамент з питань захисту персональних даних.

Згідно з статтею 11 **Закону України «Про Уповноваженого Верховної Ради України з прав людини»** та н**аказ Уповноваженого від 27.07.2012 № 7/8-12 «Про затвердження Положення про представників Уповноваженого Верховної Ради України з прав людини»** представник Уповноваженого є посадовою особою, якій делеговано визначені повноваження Уповноваженого.

Представнику Уповноваженого з питань захисту персональних даних делеговано повноваження Уповноваженого ВРУ з прав людини у сфері захисту персональних даних.

Вичерпний перелік таких повноважень викладено у статті 23 Закону[22].

Порядок проведення Уповноваженим, його представником та іншими визначеними Уповноваженим службовими особами перевірок додержання законодавства про захист персональних даних окремо визначено Порядком здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних, який було затверджено Наказом Уповноваженого від 08.01.14 № 1/2-14 (далі – Порядок)[23].

Для проведення перевірки уповноважені посадові особи (керівник Секретаріату/його заступник, представник Уповноваженого, керівник структурного підрозділу Секретаріату/його заступник, працівники Секретаріату Уповноваженого) повинні мати при собі **службове посвідчення** та **додаток до нього**, який є невід'ємною частиною посвідчення та підтверджує обсяг повноважень працівника Секретаріату.

Nota bene!

1. Посвідчення та додаток до нього є єдиними документами, які працівник Секретаріату повинен мати при собі для проведення перевірки.

2. Володільцю не надсилається жодних попереджень щодо проведення перевірки працівниками Секретаріату.

Права уповноважених посадових осіб Секретаріату Уповноваженого визначено статтею 23 Закону (див. вище) та відповідними положеннями Порядку[24].

В ході перевірки уповноважені посадові особи

---

22 Стаття 23. Повноваження Уповноваженого Верховної Ради України з прав людини у сфері захисту персональних даних Закону України «Про захист персональних даних»

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

24 П. 6. Права та обов'язки уповноваженої посадової особи та посадових осіб суб'єкта перевірки Порядку здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних

мають право доступу до будь-яких документів/інформації, які необхідні для їх проведення, і в тому числі інформації з обмеженим доступом (зокрема персональних даних), а також доступу до усіх приміщень, де здійснюється обробка персональних даних.

Єдиною умовою надання такого доступу є необхідність таких дій для здійснення контролю за забезпеченням захисту персональних даних.

Nota Bene!

Відповідно до ст. 188-40 КУПАП «невиконання законних вимог Уповноваженого Верховної Ради України з прав людини або представників Уповноваженого Верховної Ради України з прав людини тягне за собою накладення штрафу на посадових осіб, громадян – суб'єктів підприємницької діяльності від ста до двохсот неоподатковуваних мінімумів доходів громадян».

В якості невиконання законних вимог розцінюються наступні дії працівників володільця:

- Ненадання документів/інформації;
- Невчасне надання документів/інформації;
- Відмова в наданні документів/інформації;
- Недопущення до проведення перевірки;
- Ненадання доступу до приміщень;
- Ненадання доступу до інформації/ документів, що є в електронному вигляді.

За результатами проведеної перевірки відповідними посадовими особами складається акт, у якому викладається інформація щодо отриманих в ході перевірки документів та інформації, встановлених фактів та висновки щодо наявності/ відсутності порушень законодавства про захист персональних даних.

На підставі вказаних висновків приймається рішення щодо вжиття визначених Законом заходів реагування –

винесення припису або за наявності складу адміністративного правопорушення, передбаченого статтею 188-39 Кодексу України про адміністративні правопорушення, складення адміністративного протоколу.

Метою внесення припису є припинення порушення законодавства про захист персональних даних та по мірі можливості його виправлення, а також усунення обставин, що сприяли його виникненню, чи інших, що можуть призвести до його виникнення в майбутньому. З цією метою припис може містити, серед іншого, вказівки щодо: 1) зміни, 2) видалення або 3) знищення персональних даних, 4) забезпечення доступу до них, 5) надання чи 6) заборони їх надання третій особі, 7) зупинення або припинення обробки персональних даних. Вказані вимоги є зрозумілими і окремого роз'яснення не потребують. Їх метою є припинити порушення Закону (наприклад, видалити дані, що обробляються незаконно), відновити порушені права (наприклад, надати суб'єкту доступ до його персональних даних чи змінити його персональні дані, що не відповідають дійсності) або запобігти потенційним порушенням в майбутньому (наприклад, припинити обробку (зокрема, збір, зберігання та використання) персональних даних, що не є необхідними для досягнення задекларованої легітимної мети їх обробки, запровадити додаткові заходи захисту персональних даних).

Nota bene!

Відповідно до ст. 23 Закону Уповноважений має право «за підсумками перевірки, **розгляду звернення** видавати обов'язкові для виконання вимоги (приписи)», а також «складати протоколи про притягнення до адміністративної відповідальності та направляти їх до суду у випадках, передбачених законом».

Виходячи з цього, слід наголосити, що акт складається лише за результатами проведення перевірки. Якщо за результатами розгляду звернення буде виявлено правопорушення, що не вимагатиме проведення перевірки (наприклад, для підтвердження факту такого правопорушення не потрібно отримувати додаткові матеріали або достатньо отримати підтверджуючі документи чи пояснення сторін), працівниками Секретаріату буде відразу винесено припис/складено протокол.

Крім винесення припису чинним законодавством передбачено можливість складати адміністративні протоколи за вчинення певних порушень законодавства про захист персональних даних[25].

Загалом ці положення є доволі однозначними та чіткими за винятком частини четвертої, яка потребує додаткових роз'яснень. Слід наголосити, що вказане положення сформульовано доволі розпливчасто та заплутано, тому його практичне застосування пов'язане з суттєвими труднощами.

Так, частиною четвертою передбачено відповідальність за «недодержання встановленого законодавством про захист персональних даних порядку захисту персональних даних, що призвело до незаконного доступу до них або порушення прав суб'єкта персональних даних».

З об'єктивної сторони вказане положення включає два елементи, пов'язані причинно-наслідковим зв'язком:

1) недодержання встановленого законодавством про захист персональних даних порядку захисту персональних даних;

---

25 Стаття 188-[39]. Порушення законодавства у сфері захисту персональних даних

2) незаконний доступ до них або порушення прав суб'єкта персональних даних.

Слід наголосити, що в законодавстві відсутнє однозначне визначення «порядку захисту». Вище мова йшла про те, що це, перш за все, **зобов'язання володільця** вживати організаційних та технічних заходів з метою запобігання їх випадкової втрати або знищення, незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних (стаття 24 Закону). По-друге, це **зобов'язання кожного працівника** володільця та розпорядника не допускати розголошення персональних даних, які стали йому відомі у зв'язку з виконанням професійних чи службових або трудових обов'язків, так зване зобов'язання конфіденційності (стаття 10 Закону). Слід визнати, що вичерпно сформулювати поняття захисту досить складно, оскільки, як вже йшла мова вище, у кожному випадку обробки є свої особливості, які власне і обумовлюють достатній рівень захисту.

Відтак, недодержання встановленого законодавством про захист персональних даних порядку захисту персональних даних зазвичай може включати випадки розголошення працівниками персональних даних, що стали їм відомі в ході виконання обов'язків; залишення робочого місця з незавершеною сесією роботи; передачу особистого паролю доступу іншим особам; відсутність особи чи структурного підрозділу з питань захисту персональних даних; відсутність системи ідентифікації користувача перед отриманням доступу до персональних даних; відсутність обліку операцій пов'язаних з обробкою персональних даних; неорганізоване ведення документації, недостатній рівень антивірусного захисту та інше.

При цьому такі дії повинні бути в причинно-наслідковому зв'язку з незаконним доступом до персональних даних або порушенням прав суб'єкта персональних даних.

Окремо слід наголосити на певних недоліках вказаної статті. Так, Закон розрізняє поняття доступу третіх осіб та поширення/передачу третім особам (стаття 14 Закону). Порядок доступу викладено у статті 16 Закону і він базується на процедурі «запит-відповідь». У випадку, якщо персональні дані було всупереч Закону оприлюднено чи поширено (тобто

попередньо не було запиту), це вже не охоплюється поняттям доступу. Це суттєвий термінологічний недолік Закону. У всіх міжнародних документах поняття доступу використовується виключно в контексті відповідного права суб'єкта персональних даних. Коли ж мова йде про отримання персональних даних третіми особами, це характеризується як розкриття (disclosure – в національному контексті), передача (transfer – в міжнародному контексті), поширення (dissemination).

Фактично будь-яке незаконне поширення/ оприлюднення/ передача персональних даним третіми особами повинне характеризуватися як правопорушення та тягнути за собою передбачену законом відповідальність (зрештою, очевидно саме це і малося на увазі тими, хто формував текст вказаної статті КУПАП).

Однак, ще складнішою є ситуація, коли мова йде про «недодержання встановленого законодавством про захист персональних даних порядку захисту персональних даних», що призвело до «порушення прав суб'єкта персональних даних». Дійсно важко уявити, що внаслідок недодержання **порядку захисту** суб'єкт не отримав доступ до своїх персональних даних, не отримав інформацію про порядок обробки, отримав після спливу 30-ти днів інформацію про те, чи обробляються персональні дані, не зміг реалізувати своє право на заперечення про ти обробки, звернення зі скаргою до Уповноваженого та інше. Самі по собі порушення окремих прав **можуть (і повинні) бути самодостатніми правопорушеннями у сфері законодавства про захист персональних даних**, однак не зрозуміло, який зв'язок такі порушення прав можуть мати з порядком захисту персональних даних. Зазвичай вони є прямим результатом недбалості чи умисних дій володільця, спрямованих на порушення прав суб'єкта.

Для того, щоб притягнути особу за незаконне поширення/ передачу/ оприлюднення персональних даних (що по суті є найбільш серйозним правопорушенням), її дії мають кваліфікуватися як недодержання **порядку захисту,** що призвело до порушення прав суб'єкта персональних даних, а саме його права «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» (стаття 8 Закону).

На практиці довести такий причинно-наслідковий зв'язок доволі складно, це потребує встановлення більш менш чітких вимог щодо захисту персональних даних та доведення того, що саме їх порушення призвело до небажаного результату. Крім цього, це дуже сильно звужує сферу відповідальності володільця. По суті він може нести відповідальність лише за порушення порядку захисту і то лише після того, як воно призвело до якихось тяжких наслідків. В переважній же більшості випадків трапляються порушення окремих норм Закону, навіть одночасне порушення їх великої кількості, які рідко пов'язані з порушенням «порядку захисту».

При цьому виявлення таких порушень (мається на увазі тих, що не тягнуть за собою адміністративної відповідальності), як правило, завершується винесенням припису Уповноваженого, метою якого є їх усунення. У приписі фактично можна виставити будь-які вимоги з метою вдосконалення системи захисту персональних даних володільця[26]. Невиконання такого припису тягне за собою відповідальність, передбачену статтею 188-39 КУПАП (див. вище). Начебто усе в порядку. Однак насправді така система є абсолютно неефективною. Володілець незацікавлений у налагодженні належної системи захисту персональних даних із самого початку. Набагато легше дочекатися приходу з перевіркою наглядового органу (наприклад, якщо хтось направить скаргу на володільця) та виконати винесений припис. Крім того, така система становить надмірне навантаження на наглядовий орган – Уповноваженого та Секретаріат Уповноваженого. Кожна перевірка працівників Секретаріату, в ході якої було виявлено правопорушення, повинна не лише мати наслідки для володільця-об'єкта перевірки, а й стримуючий ефект щодо інших володільців. При існуючій системі цього немає.

---

26 Уповноважений має право «за підсумками перевірки, розгляду звернення видавати обов'язкові для виконання вимоги (приписи) про запобігання або усунення порушень законодавства про захист персональних даних».

Тому, видається доцільним ввести адміністративну відповідальність (нехай і мінімальну) за порушення окремих положень Закону без їх прив'язки до інших умов, як наприклад порядку захисту чи порушення прав суб'єкта.

Так, у Законі відсутня відповідальність за неповідомлення суб'єкта про збір персональних даних, незаконну обробку персональних даних (у даному випадку з порушенням статті 6, 7 та 11 Закону), обробку персональних даних на підставі згоди з порушенням основних вимог, що ставляться до неї (поінформованість, добровільність, наявність документів, що підтверджують її надання), відмову в наданні доступу суб'єкту до його персональних даних, надання неповних відомостей чи надання відповіді з порушенням визначених Законом строків, ненадання відомостей щодо порядку обробки персональних даних, ненадання відомостей про порядок доступу до персональних даних, незаконне поширення/передача персональних даних, відсутність обліку операцій, пов'язаних з обробкою персональних даних, відмову змінити/видалити персональні дані, що не відповідають дійсності, непризначення відповідальної особи, нечітке визначення її обов'язків, порушення умов щодо призначення розпорядника тощо.

Всі вказані порушення стосуються тих чи інших положень Закону, багато з яких, як вже було зазначено вище, сформульовано недостатньо чітко. Відтак, необхідно перш за все деталізувати відповідні положення Закону і вже після цього вводити відповідальність за їх порушення.

Також слід зазначити, що вказана стаття 188-39 КУПАП передбачає відповідальність за неповідомлення чи несвоєчасне повідомлення Уповноваженого ВРУ з прав людини про обробку персональних даних або про зміну відомостей, які підлягають повідомленню згідно із законом, повідомлення неповних чи недостовірних відомостей. Обов'язок повідомляти Уповноваженого передбачено статтею 9 Закону. Згідно з вказаним положенням володілець персональних даних повідомляє Уповноваженого про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, упродовж тридцяти робочих днів з дня початку такої обробки. Види обробки

персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, та категорії суб'єктів, на яких поширюється вимога щодо повідомлення, визначено Уповноваженим наказом від 8 січня 2014 року № 1/02-14, яким затверджено *Порядок повідомлення Уповноваженого ВРУ з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних при їх обробці, а також оприлюднення вказаної інформації*.

Обов'язок повідомляти та випадки, коли це необхідно робити чітко визначено Законом та наказом, а відтак, не будуть розглядатися в даному дослідженні. Принагідно слід зазначити, що станом на сьогодні відсутні випадки притягнення до адміністративної відповідальності за неповідомлення Уповноваженого.

9. ПЕРЕДАЧА ВОЛОДІЛЬЦЕМ ПЕРСОНАЛЬНИХ ДАНИХ ТРЕТІМ ОСОБАМ: ПОРЯДОК ЗДІЙСНЕННЯ ТА ТИПОВІ ПОРУШЕННЯ

Це питання є однім з ключових у законодавстві про захист персональних даних, оскільки зазвичай найбільш серйозні порушення Закону трапляються внаслідок неправомірної передачі персональних даних третім особам. Саме передача чи оприлюднення чутливої чи іншої інформації про особу може завдати найбільшої шкоди її правам. Це порушення, як вже зазначалося, може за певних умов передбачати притягнення до адміністративної відповідальності.

Будь-яка дія, внаслідок якої треті особи в той чи інших спосіб (доступ/передача/поширення/оприлюднення та ін.) ознайомлюються з персональними даними суб'єкта, повинна здійснюватися за наявності однієї з підстав, передбачених статтями 7 та 11 Закону, відповідати принципам, викладеним у статті 6 Закону. Стаття 16 доволі викладає **порядок** доступу третіх осіб до персональних даних в рамках процедури «запит – відповідь».

Виходячи із вказаних положень Закону, по-перше, будь-яка передача персональних даних повинна здійснюватися

за згодою особи або на підставі закону (див. розділ щодо принципів обробки, а також частину першу статті 16 Законуза наявності підстав, передбачених статями 7 (щодо чутливих даних) та 11 (щодо решти персональних даних) Закону. Будь-які відступи від вказаних положень допускаються виключно за умов, передбачених статтею 25 Закону.

Практика застосування Закону Уповноваженим.

Заявник зі скаргою на незаконне поширення його персональних даних психоневрологічним диспансером» (далі – диспансер). Так, за словами заявника суд розглядав справу за його позовом до лікарні. В ході судового провадження виникла необхідність в отриманні інформації щодо звернень заявника до диспансеру. З цією метою судом було направлено запит до диспансеру, у якому запитувалася інформація щодо того, чи звертався заявник в період з **2010 до травня 2013** року до диспансеру, і якщо так, то який діагноз йому було встановлено.

У відповідь на запит суду диспансер надав довідку про стан психічного здоров'я заявника, яка містила відомості про факти обстеження заявника та поставлення йому діагнозу в 2014 році, тобто у період, що виходить за межі запиту суду. Щодо запитуваного судом періоду (2010 – травень 2013 року), у довідці зазначалося про відсутність будь-яких звернень заявника в цей період часу. Зміст вказаної довідки було оголошено під час розгляду справи за позовом заявника.

У зв'язку зі зазначеними твердженнями Уповноваженим було проведено перевірку, за результатами якої було повністю підтверджено факти, викладені заявником. Вказані дії було кваліфіковано, як незаконну обробку (поширення) конфіденційної інформації (персональних даних щодо обстежень заявника диспансером та поставлених діагнозів за період з червня 2013 до грудня 2014 року).

Так, суд запитував медичну інформацію лише за період із 2010 до травня 2013 року. Відтак, у диспансеру не було підстав для надання решти інформації (за період з

червня 2013 до грудня 2014 року).
За результатом дослідження зібраних матеріалів було встановлено, що довідку, яку в подальшому було направлено до суду, було підготовлено та направлено за вказівкою керівника диспансеру, яка і засвідчила її оригінальність своїм підписом. Такі дії керівника диспансеру містили, на думку Уповноваженого, ознаки адміністративного правопорушення, передбаченого частиною четвертою статті 188-39 Кодексу України про адміністративні правопорушення, а саме – **недодержання** встановленого законодавством про захист персональних даних **порядку захисту персональних даних**, що призвело до **незаконного доступу до них** та **порушення прав** заявника (як суб'єкта персональних даних), передбачених пунктом 7 частини другої статті 8 Закону.
У зв'язку з цим працівниками Секретаріату Уповноваженого було складено щодо керівника диспансеру протокол про вчинення адміністративного правопорушення та направлено його на розгляд та прийняття рішення до суду.

Ще одним важливим моментом є вимоги щодо змісту запиту про передачу персональних даних. Так, відповідно до частини четвертої статті 16 Закону у запиті зазначаються:

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

2) найменування, місцезнаходження юридичної особи, яка подає запит, посада, прізвище, ім'я та по батькові особи, яка засвідчує запит; підтвердження того, що зміст запиту відповідає повноваженням юридичної особи (для юридичної особи – заявника);

3) прізвище, ім'я та по батькові, а також інші відомості, що дають змогу ідентифікувати фізичну особу, стосовно якої робиться запит;

4) відомості про базу персональних даних, стосовно якої подається запит, чи відомості про володільця чи розпорядника персональних даних;

5) перелік персональних даних, що запитуються;

6) мета та/або правові підстави для запиту.

Ключовим елементом у даному випадку є необхідність зазначення мети/правових підстав для запиту, оскільки лише за цими відомостями володілець зможе прийняти обґрунтоване рішення щодо доцільності передачі персональних даних. Ненадання у запиті відомостей щодо мети та підстав його направлення є формальною підставою для відмови у його задоволенні. Надання інформації (персональних даних) у відповідь на необґрунтований запит саме по собі не тягне за собою адміністративної відповідальності, якщо **підстави для надання інформації таки були.** Однак, якщо підстави для надання персональних даних відсутні, відповідних працівників володільця буде притягнуто до адміністративної відповідальності за частиною четвертою статті188-39 КУПАП.

Практика застосування Закону Уповноваженим.

В ході перевірки одного з медичних закладів працівниками Секретаріату Уповноваженого було виявлено лист Департаменту охорони здоров'я (далі – Департамент) такого змісту:

Департамент «*зобов'язує Вас, у термін до (дата), надати на адресу електронної пошти (адреса електронної пошти) списки хворих на цукровий діабет з повною або частковою втратою зору, що перебувають на обліку у підпорядкованих закладах. Форма списку додається*» (форма списку передбачала внесення до неї інформації щодо імені, прізвища, по батькові, адреси проживання, дати народження та контактного телефону особи).

Дослідження матеріалів вихідної кореспонденції засвідчило, що медичним закладом було направлено запитувану інформацію. Форма запиту та надання на нього відповіді свідчать про порушення визначеного статтею 16 Закону порядку доступу до персональних даних (див. вище). Фактично працівники медичного закладу сліпо підкорилися вказівці адміністративного органу, хоча в частині обробки наявних у них персональних даних вони є незалежним володільцем.

У ході перевірки було досліджено також фактичні підстави передачі запитаної Департаментом інформації. Для цього було проведено додаткову перевірку Департаменту, в ході якої встановлено, що збір інформації Департаментом розпочато у зв'язку з листом однієї громадської організації (далі – ГО). Вказане ГО запитувало вищезазначену медичну інформацію для того, щоб закуповувати спеціалізоване медичне обладнання для вказаних категорій осіб. Для досягнення вказаної мети воно на той момент здійснювало пошук грантових коштів.

Такі дії, на думку Уповноваженого, становлять порушення частини шостої статті 6, частини другої статті 14, частини другої статті 8, частини першої статті 24 та частини третьої статті 10 Закону (див. обґрунтування вище) як з боку працівників медичного закладу, так і з боку працівників Департаменту.

За результатом дослідження зібраних матеріалів було встановлено, що персональні дані пацієнтів було підготовлено та направлено за вказівкою керівника медичного закладу, який і підписав супровідний лист. Такі дії вказаної особи містили, на думку Уповноваженого, ознаки адміністративного правопорушення, передбаченого частиною четвертою статті 188-39 Кодексу України про адміністративні правопорушення, а саме: **недодержання** встановленого законодавством про захист персональних даних **порядку захисту персональних даних**, що призвело до **незаконного доступу до них** та **порушення прав** заявника (як суб'єкта персональних даних), передбачених пунктом 7 частини другої статті 8 Закону.

Ще одним проблемним аспектом, пов'язаним з передачею персональних даних є ідентифікація особи отримувача. Так, зазвичай для того, щоб отримати доступ до персональних даних, третім особам слід направити письмовий запит, у якому необхідно вказати відповідні реквізити (див. вище), мету/підстави запиту та засвідчити вказане власним підписом. Однак, коли мова йде про чутливу інформацію (наприклад щодо стану здоров'я, особистого життя та ін.), її надання на письмовий запит пов'язане з певними ризиками, зокрема запитувач може бути не тим, за кого себе видає. Закон не встановлює вимог щодо ідентифікації особи запитувача, однак логічно припустити, що за певних умов (сумніви щодо особи запитувача, чутливість інформації) таку ідентифікацію слід проводити. Інколи доцільно передбачити необхідність запитувача особисто з'явитися та підтвердити свою особу. Володільцям рекомендується визначати порядок отримання доступу третіх осіб до персональних даних, у якому вирішувати такі питання (див. приклад щодо ідентифікації запитувача вище).

Додаток 1. КЛЮЧОВІ РІШЕННЯ ЄВРОПЕЙСЬКОГО СУДУ З ПРАВ ЛЮДИНИ ЩОДО ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ТА ПРАВА НА ПРИВАТНІСТЬ

- «Gaskin v. The United Kingdom» (заява № 10454/83, рішення від 07/07/1989) – Обмеження доступу особи до частини документів щодо її виховання опікуном/прийомними батьками. Відсутність незалежного органу, який би розглядав клопотання щодо надання доступу до частини вказаних документів;

- «Leander v. Sweden» (заява № 9248/81) – Законність ведення таємного реєстру поліції та проведення перевірки особи за наявною у ньому інформацією перед зайняттям посади, що передбачала надання доступу до приміщень із обмеженим доступом. Законність ведення реєстру та отримання доступу до нього. Контроль за веденням реєстру.;

- «M.S. v. Sweden» (заява № 34209/92, рішення від 27/08/1997) – Передача лікарнею медичної інформації про особу на запит державного органу.;

- «Rotaru v. Romania» (заява № 28341/95, рішення від 04/05/2000) Законність ведення службою безпеки таємного реєстру. Відсутність законодавчих гарантій.;

- «I. v. Finland» (заява № 20511/03, рішення від 17/07/2008) – Відсутність обліку операцій щодо надання доступу до медичної документації заявниці, що призвело до неможливості встановлення особи, яка ймовірно поширила інформацію, що містилася у ній;

- «K.H. and Others v. Slovakia» (заява № 32881/04, рішення від 06/11/2009) – Ненадання лікарнею заявникам копій їх медичної документації;

- «L.H. v. Latvia» (заява № 52019/07, рішення від 29/04/2014) – Збір контролюючим органом інформації щодо стану здоров'я особи з метою оцінки якості наданої їй лікарнею медичної допомоги. Відсутність легітимної мети збору персональних даних. Надмірний об'єм зібраної інформації. Неврахування інтересів пацієнта.;

- «M.K. v. France» (заява № 19522/09, рішення від 18/04/2013) – Ведення реєстру відбитків пальців.;

- «Gardel v. France» (заява № 16428/05, рішення від 17/12/2009) – Ведення національними органами влади реєстру осіб, які вчинили злочини статевого характеру;

- «Uzun v. Germany» (заява № 35623/05, рішення від 02/09/2010) Спостереження за шляхами пересування особи (GPS-дані) здійснювалося законно та було пропорційним. Відсутність порушення;

- «Kennedy v. The United Kingdom» (заява № 26839/05, рішення від 18/05/2010); «Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria» (заява № 62540/00, рішення від 28/06/2007); «Klass and Others v. Germany « (рішення від 06/09/1978) – функціонування системи негласного спостереження правоохоронними органами;

- «Z. v. Finland» (заява № 22009/93, рішення від 25/02/1997) – Розкриття чутливої інформації в рішенні суду. Недостатність строків, впродовж яких обмежувався доступ до рішення суду, що містив таку інформацію;

- «Avilkina and Others v. Russia» (заява № *1585/09*, рішення від 06/06/2013) – Збір медичної інформації органами прокуратури в рамках . Законодавча невизначеність повноважень щодо збору інформації про особу. Надмірний об'єм інформації, що збирається;

- «Shimovolos v. Russia» (заява № 30194/09, рішення від 21/06/2011) – Законність функціонування таємного реєстру осіб імовірно причетних до екстремістської діяльності;

- «P.G. and J.H. v. The United Kingdom» (заява № 44787/98, рішення від 25/09/2001) Відбір, збереження та використання в ході судового провадження зразків голосу особи.;

- «S. and Marper v. The United Kingdom» (заяви № 30562/04 і 30566/04, рішення від 04/12/2008) – Законність збору та зберігання працівниками поліції відбитків пальців, профілів та зразків ДНК затриманих, підозрюваних тощо. Відсутність необхідності у зборі таких даних у порівнянні з отримуваними перевагами, неврахування індивідуальних обставин осіб, чиї дані зберігалися;

- “L.L. v. France” (no. 7508/02, ECHR 2006-XI) – використання судом в якості доказів у справі про розлучення документів, що містили відомості про стан здоров’я. Суд вказав, що у даній справі використання вказаних доказів не було необхідним.

- «Peck v. The United Kingdom» (заява № 44647/98, рішення від 28/01/2003) – Доцільність оприлюднення відеозапису, на якому видно особу після того, як вона намагалась вчинити самогубство;

- «Friedl v. Austria» (заява № 15225/89, рішення від 31/01/1995) – Законність здійснення відеофіксації силового розпуску мирного зібрання;

- «Ciubotaru v. Moldova» (заява № 27138/04, рішення від 27/04/2010) – Відмова державних органів змінити в державному реєстрі інформацію про національність особи. Покладення законодавством на особу непропорційного тягаря доведення.;

- «Garnaga v. Ukraine» (заява № 20390/07, рішення від 16/05/2013) – Закріплена на законодавчому рівні неможливість змінити по батькові особи;

- «Zaichenko v. Ukraine» (No. 2) (заява №45797/09, рішення від 26/02/2015) – Відсутність визначеної законодавством процедури збору інформації під час проведення експертизи стану психіатричного здоров’я особи в рамках провадження у справі про адміністративне правопорушення.

ДЖЕРЕЛА

1. Директива 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 року / Європейський Союз. – [Електронний ресурс]. Цит. 02.02.2018 р. Режим доступу – http://zakon4.rada.gov.ua/laws/show/994_242.
2. Європейські стандарти захисту персональних даних і е-врядування : Звіт за результатами моніторингу стану дотримання європейських стандартів захисту персональних даних при впровадженні електронних сервісів на регіональному рівні / І. М. Городиський, М. В. Бем, М.П. Левицька. – Львів: ГО «Львівський центр міжнародного права та прав людини», 2018. – 66 с.
3. Захист персональних даних: правове регулювання та практичні аспекти: науково-практичний посібник / М. В. Бем, І. М. Городиський, Г. Саттон; Європейський Союз, Рада Європи - К.: К.І.С., 2015. – 220 с.
4. Захист персональних даних у діяльності обласних державних адміністрацій: аналітичний звіт за результатами моніторингу Львівської ОДА / Городиський І.М., Левицька М.П., Бем М.В. – Львів: Львівський центр міжнародного права та прав людини, 2015. – 40 ст.
5. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28.01.1981 р. / Рада Європи. – Офіційний вісник України від 14.01.2011 р. – Офіц. Вид. – 2010/2011. – № 58. / № 58, 2010, ст. 1994 / стор. 701, стаття 85, код акту 54293/2011.
6. Медіа, конфлікт та захист персональних даних: посібник до навчального курсу / Городиський І.М., Левицька М.П., Бем М.В. – Львів: Український католицький університет; ГО «Львівський медіафорум», 2016. – 44 ст.
7. Про захист персональних даних : Закон України від 01.06.2010 р. №2297-VI / Верховна Рада України. - Офіційний вісник України від 09.07.2010 р. – Офіц. вид. – 2010. - № 49. - Стор. 199, стаття 1604, код акту 51762/2010.
8. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC / European Council // [Electronic source]. Cit. 22.02.2018. Retrieved from - http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=en

Бем М.В., Городиський І.М.

Стандарти захисту персональних даних в соціальній сфері: практичний посібник

Редагування: І.В. Олендра
Комп’ютерне верстання: П.В. Онуферко
Відповідальний за випуск: І.В. Олендра

Підписано до друку 22.03.2018 р. Формат 60х84/16
Папір офсетний. Ум.друк.арк. 13,48.
Наклад: 100 прим. Зам №22-03.2018